Abstract: Embodiments are provided herein for creating virtual networks with service chains, such as n-tier networks, in the cloud. In an embodiment, a network diagram for a virtual network is received from a user via a graphical user interface. The network diagram comprises elements that represent virtual or physical network components. The network components include switches, routers, firewalls, links, service appliances, virtual machines, servers, or other network components. Upon successfully validating the network diagram, via a validation step, the network diagram is compiled into application programming interface (API) calls ready for execution. The executed APIs are used to establish the virtual network on a physical network infrastructure. The virtual network comprises virtual network components corresponding to the elements or the network diagram.
System and Method for Creating Service Chains and Virtual Networks in the Cloud

[0001] The present application claims benefit for U.S. Non-provisional Application No. 14/191,526, filed on February 27, 2014, entitled "System and Method for Creating Service Chains and Virtual Networks in the Cloud", which application is hereby incorporated herein by reference.

TECHNICAL FIELD

[0002] The present invention relates to the field of cloud computing, and, in particular embodiments, to a system and method for creating service chains and virtual networks in the cloud.

BACKGROUND

[0003] Typical cloud networks for cloud applications and services usually consist of multiple tiers, referred to as n-tiers. Each tier hosts computers or processors that run specific functions. In addition, network tiers are usually separated from each other by network components such as firewalls and load balancers among others. An example of n-tier networks is a 3-tier network that includes a web tier, an application tier, and a database tier, coupled in sequence to a public network, e.g., the Internet. Each of the tiers resides behind a firewall which protects one tier from another. Typically, n-tier cloud networks and services are created using, command lines, preconfigured input forms, or combinations of both. Web services such as Amazon EC2™ (Elastic Compute Cloud) and OpenStack™ are examples of such approaches to build n-tier cloud networks for cloud applications and services. These web services are available for customers to build their own cloud networks and services. This includes creating security groups (SGs), each comprising a set of access control lists (ACLs). The created SGs can be applied to virtual machines (VMs) at the physical network to virtualize n-tier networks. Using such web services and similar command line and form input formats to create n-tier cloud networks and services can be challenging and time/cost demanding. There is a need for a simpler system and method for creating n-tier or virtual cloud networks and service chains, which can resolve such issues.
SUMMARY OF THE INVENTION

[0004] In accordance with an embodiment of the disclosure, a method by a cloud processing component for creating virtual networks includes receiving, from a user via a graphical user interface, a network diagram for a virtual network. The network diagram comprises elements, each one of the elements representing a network component. The method further includes validating the network diagram, and upon successful validation of the network diagram, compiling the network diagram into application programming interface (API) calls. The API calls are then executed. Using the executed the API calls, the virtual network is established according to the network diagram. The virtual network comprises virtual network components corresponding to the elements of the network diagram.

[0005] In accordance with another embodiment of the disclosure, a method by a user for creating virtual networks includes entering, using a graphical user interface of a cloud computing platform, a network diagram representing a virtual network. The network diagram comprises elements, each one of the elements representing a network component. The network diagram enables the cloud computing platform to establish, using application programming interface (API) calls, the virtual network. The virtual network comprises virtual network components corresponding to the elements of the network diagram.

[0006] In accordance with yet another embodiment of the disclosure, a network component for creating virtual networks includes at least one processor and a non-transitory computer readable storage medium storing programming for execution by the at least one processor. The programming includes instructions to receive, from a user via a graphical user interface, a network diagram for a virtual network. The network diagram comprises elements, each one of the elements representing a physical network component. The programming includes further instructions to validate the network diagram, and upon successful validation of the network diagram, compile the network diagram into API calls. The network component is further configured to execute the API calls, and establish, using the executed the API calls, the virtual network according to the network diagram. The virtual network comprises virtual network components corresponding to the elements or the network diagram.

[0007] The foregoing has outlined rather broadly the features of an embodiment of the present invention in order that the detailed description of the invention that follows may be better
understood. Additional features and advantages of embodiments of the invention will be described hereinafter, which form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and specific embodiments disclosed may be readily utilized as a basis for modifying or designing other structures or processes for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawing, in which:

[0009] Figure 1 illustrates an example of a 3-tier cloud network;

[0010] Figure 2 illustrates an embodiment for creating n-tier networks with service chains in the cloud;

[0011] Figure 3 illustrates an embodiment of creating n-tier networks via a graphical user interface;

[0012] Figure 4 illustrates an embodiment of a method for creating n-tier networks; and

[0013] Figure 5 is a diagram of a processing system that can be used to implement various embodiments.

[0014] Corresponding numerals and symbols in the different figures generally refer to corresponding parts unless otherwise indicated. The figures are drawn to clearly illustrate the relevant aspects of the embodiments and are not necessarily drawn to scale.
DETAILED DESCRIPTION OF illustrative embodiments

[0015] The making and using of the presently preferred embodiments are discussed in detail below. It should be appreciated, however, that the present invention provides many applicable inventive concepts that can be embodied in a wide variety of specific contexts. The specific embodiments discussed are merely illustrative of specific ways to make and use the invention, and do not limit the scope of the invention.

[0016] Figure 1 shows an example of a 3-tier network 100 that includes a web tier 110, an application tier 120, and a database tier 130. The tiers face a public network 140, for example the Internet. Each tier hosts computers, processors, or servers that run specific functions of the corresponding tier. Each tier also resides behind a firewall component or function that protects the corresponding tier from external components (other tiers and the public network). Typically, software tools such as Microsoft Visio™, or network planning tools such as OpNET™ can be used to draw a network diagram of the 3-tier or other n-tier networks. The diagram is used as a guideline by the user (e.g., a system engineer) to select and connect suitable network equipment and servers for establishing the n-tier network. Typically, to build n-tier virtual networks in the cloud, element groups, such as security groups (SGs) by Amazon, are created using a software tool, such as EC2™. Policy rules are then added, e.g., via access control lists (ACLs) for the traffic of each SG. For example, for a 2-tier network, two SGs, WebServerSG and DBServerSG, are created. ACLs are then added for both inbound and outbound traffic for each SG. Virtual machines (VMs) are then established for each tier, and used to apply the SGs.

[0017] With the rapid adoption of cloud computing, customers need to be able to conveniently construct n-tier networks in the cloud to migrate or mimic their on-premise environment. However, current cloud computing platforms such as Amazon EC2™ and OpenStack™ include limited user interfaces for creating virtual networks, such as using input forms and line commands. Embodiments are provided herein for creating service chains and virtual networks, such as n-tier networks, in the cloud. The embodiments include systems and methods for building virtual networks in the cloud using user-friendly network diagram drawing methodology and user interface. Using the schemes herein, a cloud computing provider can provide a user-friendly self-service that allows its customers to easily create virtual networks in the cloud, which mimic their existing on-premise physical networks.

[0018] Figure 2 shows an embodiment 200 for creating virtual networks, such as n-tier networks with service chains in the cloud. A user can first log into a cloud management
platform/system via a cloud portal, e.g., a web site or service. The user then draws a network diagram representing the n-tier network. Each of the tiers provides a service. In this scenario, 3 services, including a database service, an application service, and a web service, are linked in that sequence, hence forming a service chain. The network diagram can include any suitable network components that mimic or correspond to network components, such as switches, routers, other service appliances, links, and/or other network components. The network diagram also reflects the actual intended topology of the virtual network, such as the hierarchy/sequence and interconnections between the different components. The process of drawing a network diagram is interactive in that the system may ask the user for input and also provide feedback according to user's actions.

[0019] The network diagram is drawn using a graphical user interface (GUI) that is part of the cloud management platform/system. The GUI can be provided by a software tool or web service. After submitting the network diagram which represents the n-tier network, the system can validate the network diagram. If the network diagram passes the validation process, the system compiles the network diagram into application programming interface (API) calls. The API calls are then executed by the system to configure one or more underlying physical networks to establish a virtual n-tier network according to the network diagram of the user. Thus, the diagram components are mapped, essentially one-to-one, into corresponding virtual network components. The system is aware of each of the components or elements of the diagram and is capable to map the element to a corresponding virtual element. The virtual network provides network connectivity and also guarantees policy enforcement. The virtual network can be established according to the available virtualization technology provided by the system or the physical networks, such as a virtual local area network (VLAN).

[0020] In an embodiment, each user or a group of users (e.g., in an enterprise) initially get (e.g., via purchase) or is initially assigned a resource pool comprising a maximum quantity of available resources for the user or group to establish virtual or cloud based n-tier networks. For example, the resource pool can include a maximum number of VLANs, switch ports, forwarding entries, bandwidth, storage size, and/or other network resources which are available to the user or group. The total available resources in a resource pool assigned to a user or a group of users can also be divided (reassigned) to other individual users or groups. Accordingly, each user or group uses the corresponding designated resources for building corresponding virtual n-tier networ
Figure 3 shows an embodiment scheme 300 of creating virtual networks, such as n-tier networks, via a graphical user interface. As described above, the graphical interface is presented to the user (after signing in) by a cloud system. As an example, the user creates 3 logical networks (a 3-tier virtual network), comprising web servers, application servers, and database servers that connected in sequence to the Internet (or a public network) in that order. The 3 tiers or logical networks are created by drawing a corresponding diagram with a box or element for each component, as shown in Figure 3. The elements also include firewalls between the logical networks and links between the elements, as placed by the user. This completes the network diagram. The user can then submit the diagram to the system to build his n-tier network in the cloud. The cloud system then compiles the network diagram into API calls and executes the API calls automatically. The automatically executed API calls configure the underlying physical network(s) to create a 3-tier virtual network. The created virtual network provides network connectivity and guarantee policy enforcement.

Figure 4 illustrates an embodiment of a method 400 for creating virtual networks, such as n-tier networks. At step 410, a pool of resources is assigned to a user or group of users. At step 420, a network diagram of a n-tier or other virtual network is received from a user via a graphical user interface and a cloud portal. At step 430, the system validates the network diagram. The validation process includes the verification that the user has not exceeded the allowed resources according to the assigned resource pool. Other validation rules may apply, such as network policy rules. At decision step 435, the system checks whether the network diagram is valid. If the network diagram is valid, then the method 400 proceeds to step 450. Otherwise, at step 440, a feedback is sent to the user to correct the network diagram. The method 200 then returns to step 430 to wait for user input. Alternatively, at step 450, the network diagram is compiled into API calls. At step 460, the APIs are executed to configure the underlying physical network to establish a virtual network with (virtual) components that map the elements of the user network diagram.

Figure 5 is a block diagram of an exemplary processing system 500 that can be used to implement various embodiments. The processing system is part of a cloud platform/system for creating n-tier networks with service chains in the cloud as described above. The processing system 500 may comprise a processing unit 501 equipped with one or more input/output devices, such as a speaker, microphone, mouse, touchscreen, keypad, keyboard, printer, display, and the like. The processing unit 501 may include a central processing unit (CPU) 510, a mem' \$_5$ storage device 530, a video adapter 540, and an Input/Output (I/O) interface \$_7$ to a bus. The bus may be one or more of
any type of several bus architectures including a memory bus or memory controller, a peripheral bus, a video bus, or the like.

[0024] The CPU 510 may comprise any type of electronic data processor. The memory 520 may comprise any type of system memory such as static random access memory (SRAM), dynamic random access memory (DRAM), synchronous DRAM (SDRAM), read-only memory (ROM), a combination thereof, or the like. In an embodiment, the memory 520 may include ROM for use at boot-up, and DRAM for program and data storage for use while executing programs. The mass storage device 530 may comprise any type of storage device configured to store data, programs, and other information and to make the data, programs, and other information accessible via the bus. The mass storage device 530 may comprise, for example, one or more of a solid state drive, hard disk drive, a magnetic disk drive, an optical disk drive, or the like.

[0025] The video adapter 540 and the I/O interface 590 provide interfaces to couple external input and output devices to the processing unit. As illustrated, examples of input and output devices include a display 560 coupled to the video adapter 540 and any combination of mouse/keyboard/printer 570 coupled to the I/O interface 590. Other devices may be coupled to the processing unit 501, and additional or fewer interface cards may be utilized. For example, a serial interface card (not shown) may be used to provide a serial interface for a printer.

[0026] The processing unit 501 also includes one or more network interfaces 550, which may comprise wired links, such as an Ethernet cable or the like, and/or wireless links to access nodes or one or more networks 580. The network interface 550 allows the processing unit 501 to communicate with remote units via the networks 580. For example, the network interface 550 may provide wireless communication via one or more transmitters/transmit antennas and one or more receivers/receive antennas. In an embodiment, the processing unit 501 is coupled to a local-area network or a wide-area network for data processing and communications with remote devices, such as other processing units, the Internet, remote storage facilities, or the like.

[0027] While several embodiments have been provided in the present disclosure, it should be understood that the disclosed systems and methods might be embodied in many other specific forms without departing from the spirit or scope of the present disclosure. The present examples are to be considered as illustrative and not restrictive, and the intention is not to be limited to the details give -example, the various elements or...
components may be combined or integrated in another system or certain features may be omitted, or not implemented.

In addition, techniques, systems, subsystems, and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other items shown or discussed as coupled or directly coupled or communicating with each other may be indirectly coupled or communicating through some interface, device, or intermediate component whether electrically, mechanically, or otherwise. Other examples of changes, substitutions, and alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.
WHAT IS CLAIMED IS:

1. A method by a cloud processing component for creating virtual networks, the method comprising:
   - receiving, from a user via a graphical user interface, a network diagram for a virtual network, wherein the network diagram comprises elements, each one of the elements representing a network component;
   - validating the network diagram;
   - upon successful validation of the network diagram, compiling the network diagram into application programming interface (API) calls;
   - executing the API calls; and
   - establishing, using the executed the API calls, the virtual network according to the network diagram, wherein the virtual network comprises virtual network components corresponding to the elements or the network diagram.

2. The method of claim 1 further comprising assigning a pool of resources to the user, wherein validating the network diagram includes verifying that the network diagram does not use more resources than is assigned in the resource pool for the user.

3. The method of claim 1, wherein receiving the network diagram via the graphical user interface includes providing feedback to the user according to actions of the user.

4. The method of claim 1 further comprising upon unsuccessful validation of the network diagram, providing feedback to the user indicating missing or incorrect input in the network diagram.

5. The method of claim 1, wherein establishing the virtual network includes mapping each one of the elements of the network diagram to one corresponding component of the virtual network components in accordance with a topology of the network diagram.

6. The method of claim 1, wherein establishing the virtual network using the executed the API calls includes providing network connectivity and policy enforcement.

7. The method of claim 1, wherein the virtual network is a virtual local area network (VLAN).

8. The method of claim 1, wherein the virtual network includes a sequence of network tiers, and wherein the elements of the network diagram include blocks representing virtual machines (VMs) or servers for each one of the tier networks, and firewalls that separate the network tiers.
9. The method of claim 1, wherein the network component represented by each one of
the elements of the network diagram is a switch, a router, a firewall, a link, or a service
appliance.
10. A method by a user for creating virtual networks, the method comprising:
entering, using a graphical user interface of a cloud computing platform, a network
diagram representing a virtual network, the network diagram comprising elements, each one
of the elements representing a network component,
wherein the network diagram enables the cloud computing platform to establish, using
application programming interface (API) calls, the virtual network, and
wherein the virtual network comprises virtual network components corresponding to
the elements of the network diagram.
11. The method of claim 10, wherein the virtual network includes a sequence of network
tiers, and wherein the elements of the network diagram include blocks representing virtual
machines (VMs) or servers for each one of the tier networks, and firewalls that separate the
network tiers.
12. The method of claim 10 further comprising accessing the graphical user interface via a
web portal.
13. The method of claim 10 further comprising selecting the elements of the network
diagram in accordance with a pool of resources assigned to the user.
14. The method of claim 10, wherein entering the network diagram using the graphical
user interface includes receiving feedback from the cloud computing platform according to
actions of the user.
15. A network component for creating virtual networks, the network component
comprising:
at least one processor; and
a non-transitory computer readable storage medium storing programming for
execution by the at least one processor, the programming including instructions to:
receive, from a user via a graphical user interface, a network diagram for a virtual
network, wherein the network diagram comprises elements, each one of the elements
representing a physical network component;
validate the network diagram;
upon successful validation of the network diagram, compile the network diagram
into application programming interface (API) calls;
execute the API calls; a
establish, using the executed the API calls, the virtual network according to the
network diagram, wherein the virtual network comprises virtual network components
corresponding to the elements or the network diagram.

16. The network component of claim 15, wherein the programming includes further
instructions to assign a pool of resources to the user, wherein validating the network diagram
includes verifying that the network diagram does not use more resources than is assigned in
the resource pool for the user.

17. The network component of claim 15, wherein the instructions to establish the virtual
network include instructions to map each one of the elements of the network diagram to one
corresponding component of the virtual network components in accordance with a topology
of the network diagram.

18. The network component of claim 15, wherein the instructions to establish the virtual
virtual network using the executed the API calls include instructions to provide network
connectivity and policy enforcement.

19. The network component of claim 15, wherein the virtual network includes a database
tier, an application tier, and a web tier inter-coupled in sequence via links, wherein the web
tier is further coupled to a public network, and wherein the virtual network further includes a
firewall on each of the links between the database tier, the application tiers, and the web tier.

20. The network component of claim 15, wherein the graphical user interface is accessible
via a web portal.
FIG. 2

1. USER LOGS INTO A CLOUD MANAGEMENT PLATFORM

2. USER DRAWS A NETWORK DIAGRAM COMPRISING SWITCHES, ROUTERS, SERVICE APPLIANCES, LINKS, AND/OR OTHER NETWORK COMPONENTS

3. NETWORK DIAGRAM IS COMPILED INTO API CALLS

4. API CALLS ARE EXECUTED TO CONFIGURE PHYSICAL NETWORKS, RESULTING IN A VIRTUAL NETWORK PROVIDING BOTH NETWORK CONNECTIVITY AND POLICY ENFORCEMENT

CLOUD PORTAL

GUI

API CALLS
1. User creates a logical network comprising web servers, application servers, and database servers, respectively, along with a public network, e.g., the Internet.

2. User places a firewall in front of each logical network and then links the networks together.

3. The system compiles the network diagram into APIs, calls which then automatically configures the underlying physical network in the cloud to create a 3-tier virtual network. The created virtual network provides network availability and guarantee of policy enforcement.
ASSIGN A POOL OF RESOURCES TO A USER OR GROUP OF USERS

RECEIVE A NETWORK DIAGRAM FOR A N-TIER OR OTHER VIRTUAL NETWORK FROM A USER VIA A GRAPHICAL USER INTERFACE AND A CLOUD PORTAL

VALIDATE THE NETWORK DIAGRAM. THE VALIDATION PROCESS INCLUDES THE VERIFICATION THAT THE USER HAS NOT EXCEEDED THE ALLOWED RESOURCES ACCORDING TO THE ASSIGNED RESOURCE POOL

IS THE NETWORK DIAGRAM VALID?

NO
SEND FEEDBACK TO THE USER

YES

COMPILE THE NETWORK DIAGRAM INTO API CALLS

EXECUTE THE APIs TO CONFIGURE THE UNDERLYING PHYSICAL NETWORK TO ESTABLISH A VIRTUAL NETWORK WITH VIRTUAL COMPONENTS MAPPING TO THE USER PROVIDED DIAGRAM

FIG. 4
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
H04L 12/915(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
CNPAT; WPI; EPDOC; CNKI: virtual network, graphical user interface, network, diagram, cloud, computer, resource pool, API, establish+, creat+, set, database, graphical, draw, validat+, compil+, component

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category*</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>CN 102904794 A (BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) description paragraphs [0006]-[0016]</td>
<td>1-20</td>
</tr>
<tr>
<td>A</td>
<td>US 2012151371 A1 (WYSE TECHNOLOGY INC.) 14 June 2012 (2012-06-14) the whole document</td>
<td>1-20</td>
</tr>
<tr>
<td>A</td>
<td>CN 103226489 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 31 July 2013 (2013-07-31) the whole document</td>
<td>1-20</td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of Box C.  See patent family annex.

* Special categories of cited documents:
  "A" document defining the general state of the art which is not considered to be of particular relevance
  "E" earlier application or patent but published on or after the international filing date
  "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  "O" document referring to an oral disclosure, use, exhibition or other means
  "P" document published prior to the international filing date but later than the priority date claimed
  "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
  "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be regarded as involving an inventive step when the document is taken alone
  "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
  "&" document member of the same patent family

Date of the actual completion of the international search
24 April 2015

Date of mailing of the international search report
06 May 2015

Name and mailing address of the ISA/CN
STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA(ISACN)
6, Xitucheng Rd., Jinmen Bridge, Haidian District, Beijing 100088, China

Authorized officer
XING,Yunfeng

Facsimile No. (86-10)62019451
Telephone No. (86-10)62413374

Form PCT/ISA/210 (second sheet) (July 2009)
<table>
<thead>
<tr>
<th>Patent document cited in search report</th>
<th>Publication date (day/month/year)</th>
<th>Patent family member(s)</th>
<th>Publication date (day/month/year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN 102904794 A</td>
<td>30 January 2013</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>CN 103430123 A</td>
<td></td>
<td>CN 103300123 A</td>
<td>04 December 2013</td>
</tr>
<tr>
<td>CN 103226489 A</td>
<td>31 July 2013</td>
<td>US 2013198740 A1</td>
<td>01 August 2013</td>
</tr>
</tbody>
</table>