Infrastructure as Code (1 of 2)

- **Software defined network (SDN)**
  - An SDN virtualizes parts of the physical network so that it can be more quickly and easily reconfigured
  - This is accomplished by separating the *control plane* from the *data plane*
  - If traffic needs to flow through the network:
    - It receives permission from the SDN controller, which verifies the communication is permitted by the network policy of the enterprise
    - Once approved, the SDN controller computes a route for the flow to take and adds an entry for that flow in each of the switches along the path

Infrastructure as Code (2 of 2)

- Software-Defined Visibility (SDV)
  - **Software-defined visibility (SDV)** is a framework that allows users to create programs in which critical security functions can be automated
  - SDV allows network administrators to automate multiple functions in a network infrastructure including:
    - Dynamic response to detected threat patterns
    - Adjustments to traffic mode configurations for in-line security tools
    - Additional IT operations-management functions and capabilities

Security Concerns for Virtual Environments (1 of 3)

- Security-related advantages of virtualization:
  - Test latest security updates by downloading on a virtual machine before installing on production computers
  - A *snapshot* of a particular state of a virtual machine can be saved for later use
  - Testing the existing security configuration *(security control testing)* can be performed using a simulated network environment
  - VMs can promote security segregation and isolation
  - A suspicious program can be loaded into an isolated virtual machine and executed *(sandboxing)*
    - If the program is malware, only the virtual machine will be impacted

Security Concerns for Virtual Environments (2 of 3)

- Security concerns for virtualized environments:
  - Not all hypervisors have the necessary security controls to keep out attackers
  - Existing security tools were designed for single physical servers
  - VMs must be protected from both outside networks and other VMs on the same physical computer
  - VMs may be able to "escape" from the contained environment and directly interact with the host OS
    - Important to have **virtual machine escape protection**
- *Virtual machine sprawl* is the widespread proliferation of VMs without proper oversight or management
- Combating VM sprawl is called **virtual machine sprawl avoidance**
  - Installing a virtual machine manager can help

Security Concerns for Virtual Environments (3 of 3)

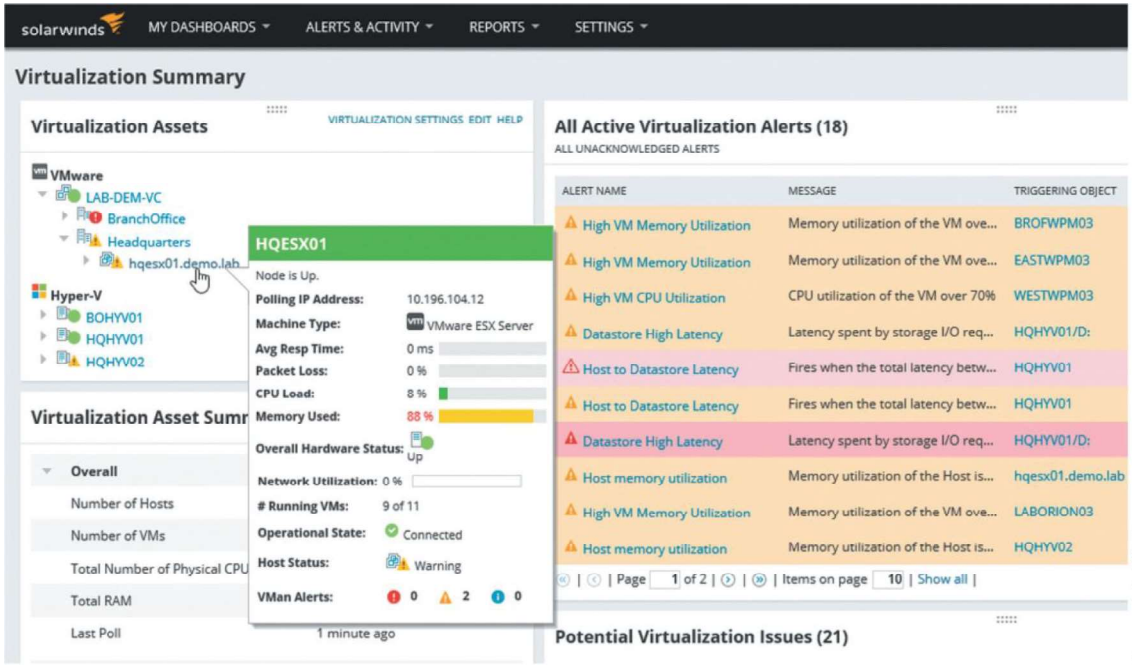

Figure 10-10 Virtual machine manager

Figure 10-10 Virtual machine manager

Knowledge Check Activity 2

What virtualization technology separates the control plane from the data plane on networking devices such as switches and routers?

a. SDV
b. Hypervisor
c. Containers
d. SDN

Knowledge Check Activity 2: Answer

What virtualization technology separates the control plane from the data plane on networking devices such as switches and routers?

Answer: d. SDN

A software-defined network (SDN) virtualizes parts of the physical network by separating the control plane from the data plane.

Secure Network Protocols

- Common secure network protocols include:
  - Simple Network Management Protocol (SNMP)
  - Domain Name System (DNS) Security Extensions
  - File Transfer Protocol
  - Secure email protocols
  - Lightweight Directory Access Protocol (LDAP)
  - Internet Protocol version 6 (IPv6)

Simple Network Management Protocol (SNMP)

- SNMP is used to manage network equipment and is supported by most network equipment manufacturers
- It allows administrators to remotely monitor, manage, and configure network devices
- SNMP functions by exchanging management information between network devices
- Each SNMP-managed device has an agent or a service
  - Listens for and executes commands
- Agents are password protected
  - Password is known as a *community string*
- Security vulnerabilities were present in SMNP versions 1 and 2
  - Version 3 uses usernames and passwords along with encryption to address vulnerabilities

Domain Name System Security Extensions (DNSSEC)

- DNS is often the focus of attacks
  - DNS poisoning and DNS hijacking are examples
- These attacks can be thwarted by using **Domain Name System Security Extensions** (**DNSSEC**)
  - DNSSEC adds additional resource records and message header information which can be used to verify the requested data has not been altered in transmission
- Using asymmetric cryptography, a private key that is specific to a zone is used in encrypting a hash of a set of resource records
  - Which is then used to create the digital signature to be stored in the resource record

File Transfer Protocol (1 of 2)

- File transfer protocol (FTP) is an unsecure protocol used to connect to an FTP server in order to transfer files
- Methods for using FTP on local host computer
  - *Using an FTP client*
  - *From a command prompt*
  - *Using a web browser*
- FTP vulnerabilities include:
  - FTP does not use encryption
  - Files transferred using FTP are vulnerable to man-in-the-middle attacks

File Transfer Protocol (2 of 2)

- There are two options for secure transmissions over FTP
  - FTP Secure (FTPS) uses SSL or TLS to encrypt commands sent over the control port (port 21)
    - The data port (port 20) may not be encrypted
  - Secure FTP (SFTP)
    - Uses only a single TCP port instead of two ports
    - All data and commands are encrypted

Secure Email Protocols

- Earlier email systems use two TCP/IP protocols to send and receive messages:
  - Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP)
- IMAP (Internet Mail Access Protocol) is a more recent and advanced email system
- As a means of security, a *mail gateway* monitors emails for unwanted content and prevents these messages from being delivered
- A mail gateway can automatically and transparently encrypt outbound email messages

Lightweight Directory Access Protocol (LDAP)

- A **directory service** is a database stored on the network that contains information about users and network devices
  - The directory service also keeps track of all the resources on the network and a user's privileges to those resources and grants or denies access based on the directory service information
- **Lightweight Directory Access Protocol** (**LDAP**) makes it possible for almost any application running on any computer platform to obtain directory information
- A weakness of LDAP is that it can be subject to **LDAP injection attacks**
  - This may allow an attacker to construct LDAP statements based on user input statements
- The defense against LDAP injection attacks is to examine all user input before processing

Internet Protocol Version 6 (IPv6)

- IPv6 addresses weaknesses of IPv4 and also provides other significant improvements
  - IPv6 increases the number of available addresses
- IPv6 has enhanced security features:
  - IPv6 can implement end-to-end encryption
    - This makes man-in-the-middle attacks significantly more difficult
  - IPv6 supports more secure name resolution
    - The Secure Neighbor Discovery (SEND) protocol can send cryptographic confirmation that an endpoint is who it claims to be
    - This makes ARP poisoning more difficult

Knowledge Check Activity 3

Which type of networking service is potentially susceptible to LDAP injection attacks?

a. Directory service
b. Domain name service
c. Web service
d. Mail service

Knowledge Check Activity 3: Answer

Which type of networking service is potentially susceptible to LDAP injection attacks?

Answer: a. Directory service

Lightweight Directory Access Protocol (LDAP) is a protocol for using and maintaining directory services which is a database stored on a network that contains information about users and other network services.

Self-Assessment

Rate your competence of the following module objectives on a scale of 1 to 5 where 5 indicates you have full confidence in your competence of that objective and 1 indicates you have very little to no confidence in your competence of that objective. After you self-score, consider why some topics were easier for you to digest than others and review any objective you are not confident about.

1. Define the cloud and explain how it is used and managed

2. Explain virtualization

3. Describe cloud and virtualization security controls

4. List different secure network protocols

Summary (1 of 2)

- Cloud computing is a popular and flexible approach to computing resources
- A public cloud is one in which the services and infrastructure are offered to all users with access provided remotely through the Internet
- On-premises is computing resources located on the campus of the organization while off-premises is a computing resource hosted and supported by a third party
- There are many elements that make up a cloud architecture: a thin client, a transit gateway, and a serverless infrastructure
- Cloud computing service models include: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Anything as a Service (XaaS)
- Cloud computing has several potential security issues

Summary (2 of 2)

- While securing the functional areas of the cloud is important, an area often overlooked is application security or protecting applications
- Virtualization is a means of managing and presenting computer resources by function without regard to their physical layout or location
- Instances of virtualization are sometimes referred to as infrastructure as code
- There are several secure network protocols that are used today: SNMP, DNSSEC, FTPS, and SFTP
- Electronic email systems that are in use today: SMTP/POP3 and IMAP