Server and system administration

Server and system administrators perform a variety of important tasks in a network environment. Typical server and system administration tasks include:

- Account provisioning and deprovisioning
- Managing account permissions
- Installing and maintaining server software
- Maintaining and optimizing servers, applications, databases (may be assigned to a database administrator), network devices (may be assigned to a network administrator), and security devices (may be assigned to a security administrator)
- Installing security patches
- Managing system and data backup and recovery
- Monitoring network communication and server logs
- Troubleshooting and resolving server and system issues

Identity and access management

Identity and access management (IAM) provides authentication, authorization, and access control functions. IAM tools provide control for the provisioning, maintenance, and operation of identities — including users, devices, and services — and the level of access to network, data center, and cloud resources that different identities are permitted. Authentication is the process of verifying an identity based on one of (single-factor authentication) or a combination of (multi-factor authentication) the following three factors:

- **Something you know** (such as a password or PIN)
- **Something you have** (such as a security token or authenticator app)
- **Something you are** (biometrics, such as a fingerprint or retina pattern)

Multi-factor authentication (MFA) is becoming more common as organizations recognize the inherent weaknesses associated with single-factor authentication techniques such as passwords and PINs. MFA typically requires a username (or user ID), password, and a one-time passcode sent to a smartphone via SMS text, authenticator app (such as Microsoft Authenticator or Google Authenticator), or a hardware token. The one-time passcode is only valid for a limited period of time (typically one to five minutes) and only for a single login session. Many organizations implement MFA with dynamic policies to limit the number of times users are prompted for MFA. For example, the organization might require MFA only once every five days or only if the user is authenticating from a different IP address than usual.

Palo Alto Networks Cybersecurity Academy

Effective IAM requires organizations to implement well-defined processes for account provisioning/deprovisioning, role-based access control (RBAC), privilege management, and access reviews to ensure user accounts (and other directory objects) are promptly created and disabled/deleted, least privilege access is enforced, and good user/network hygiene is maintained.

Directory services

A directory service is a database that contains information about users, resources, and services in a network. The directory service associates users and network permissions to control who has access to which resources and services on the network. Directory services include:

Active Directory. A centralized directory service developed by Microsoft for Windows networks to provide authentication and authorization of users and network resources. Active Directory uses Lightweight Directory Access Protocol (LDAP), *Kerberos*, and the Domain Name System (DNS).

Lightweight Directory Access Protocol (LDAP). An IP-based client-server protocol that provides access and manages directory information in TCP/IP networks.

Key Terms

Kerberos is an authentication protocol in which tickets are used to identify network users.

Vulnerability and patch management

New software vulnerabilities and exploits are discovered all the time, requiring diligent software patch management by system and security administrators in every organization.

However, patch management protects an organization's endpoints only after a vulnerability has been discovered and the patch installed. Delays of days, weeks, or longer are inevitable because security patches for newly discovered vulnerabilities must be developed, distributed, tested, and deployed. Although patch management is an important aspect of any information security program, like signature-based anti-malware detection, it is an endless race against time that offers no protection against zero-day exploits.

Organizations should also proactively perform regular vulnerability assessments to identify, evaluate, quantify, and prioritize security weaknesses in their applications and systems. Vulnerability assessments may consist of port scans, vulnerability scans, and/or penetration tests.

Configuration management

Configuration management is the formal process used by organizations to define and maintain standard configurations for applications, devices, and systems throughout their lifecycle. For example, a particular desktop PC model may be configured by an organization with specific security settings, such as enabling whole disk encryption and disabling USB ports. Within the desktop operating system, security settings such as disabling unneeded and risky services (for example, FTP and Telnet) may be configured. Maintenance of standard configurations on applications, devices, and systems used by an organization helps reduce risk exposure and improve security posture.

Palo Alto Networks Cybersecurity Academy

Structured host and network troubleshooting

A network or segment of a network that goes down could have a negative impact on your organization or business. Network administrators should use a systematic process to troubleshoot network problems when they occur to restore the network to full production as quickly as possible without causing new issues or introducing new security vulnerabilities. The troubleshooting process performed by a network administrator to resolve network problems quickly and efficiently is a skill that is highly sought after in IT.

Two of the most important troubleshooting tasks a network administrator performs occur long before a network problem occurs: baselining and documenting the network.

A baseline provides quantifiable metrics that are periodically measured with various network performance monitoring tools, protocol analyzers, and packet sniffers. Important metrics might include application response times, server memory and processor utilization, average and peak network throughput, and storage input/output operations per second. These baseline metrics provide an important snapshot of normal network operations to help network administrators identify impending problems, troubleshoot current problems, and know when a problem has been fully resolved.

Network documentation should include logical and physical diagrams, application data flows, change management logs, user and administration manuals, and warranty and support information. Network baselines and documentation should be updated any time a significant change to the network occurs and as part of the change management process of an organization.

Many formal multistep troubleshooting methodologies have been published, and organizations or individual network administrators may have their own preferred method. Generally speaking, troubleshooting consists of these steps:

1. Discover the problem.
2. Evaluate the system configuration against the baseline.
3. Track the possible solutions.
4. Execute a plan.
5. Check the results.
6. Verify the solution. (If unsuccessful, return to Step 2. If successful, go to Step 7.)
7. Deploy the positive solution.

Troubleshooting host and network connectivity problems typically starts with analyzing the scope of the problem and identifying the devices and services that are affected. Problems with local hosts are typically much easier to assess and remedy than problems that affect a network segment or service. For an individual device that loses network connectivity, the problem sometimes can be easily resolved by simply restarting the device. However, problems with integrated or shared services (for example, web or file services) can be complex, and restarting a service or rebooting a device may actually compound the problem. Connectivity problems may be intermittent or difficult to trace, so it's important that your troubleshooting processes follow an approved or standardized methodology.

Palo Alto Networks Cybersecurity Academy

The OSI model provides a logical model for troubleshooting complex host and network issues. Depending on the situation, you might use the bottom-up, top-down, or divide-and-conquer approach discussed in the following paragraphs when you use the OSI model to guide your troubleshooting efforts. In other situations, you might make an educated guess about the source of the issue and begin investigating at the corresponding layer of the OSI model, or use the substitution method (replacing a bad component with a known good component) to quickly identify and isolate the cause of the issue.

When you use a bottom-up approach to diagnose connectivity problems, you begin at the Physical layer of the OSI model by verifying network connections and device availability. For example, a wireless device may have power to the antenna or transceiver temporarily turned off. Or a wireless access point may have lost power because a circuit breaker was tripped offline or a fuse was blown. Similarly, a network cable connection may be loose, or the cable may be damaged. Thus, before you begin inspecting service architectures, you should start with the basics: Confirm physical connectivity.

Moving up to the Data Link layer, you verify data link architectures, such as compatibility with a particular standard or frame type. Although Ethernet is a predominant LAN network standard, devices that roam (such as wireless devices) sometimes automatically switch between Wi-Fi, Bluetooth, and Ethernet networks. Wireless networks usually have specified encryption standards and keys. Connectivity may be lost because a network device or service has been restored to a previous setting, and the device is not responding to endpoint requests that are using different settings. Firewalls and other security policies may also be interfering with connection requests. You should never disable firewalls, but in a controlled network environment with proper procedures established, you may find that temporarily disabling or bypassing a security appliance resolves a connectivity issue. The remedy then is to properly configure security services to allow the required connections.

Various connectivity problems may also occur at the Network layer. Important troubleshooting steps include confirming proper network names and addresses. Devices may have improperly assigned IP addresses that are causing routing issues or IP address conflicts on the network. A device may have an improperly configured IP address because it cannot communicate with a DHCP server on the network. Similarly, networks have different identities, such as wireless SSIDs, domain names, and workgroup names. Another common problem exists when a particular network has conflicting names or addresses. Issues with DNS name resolvers may be caused by DNS caching services or connection to the wrong DNS servers. *Internet Control Message Protocol* (ICMP) is used for network control and diagnostics at the Network layer of the OSI model. Commonly used ICMP commands include **ping** and **traceroute**. These two simple but powerful commands (and other ICMP commands and options) are some of the most commonly used tools for troubleshooting network connectivity issues. You can run ICMP commands in the command-line interface on computers, servers, routers, switches, and many other networked devices.

Key Terms

Internet Control Message Protocol (ICMP) is an internet protocol used to transmit diagnostic messages.

At the Transport layer, communications are more complex. Latency and network congestion can interfere with communications that depend on timely acknowledgments and handshakes. Time-to-live (TTL) values sometimes have to be extended in the network service architecture to allow for slower response times during peak network traffic hours. Similar congestion problems can occur when new services are added to an existing network or when a local device triggers a prioritized service, such as a backup or an antivirus scan.

Session layer settings can also be responsible for dropped network connections. For example, devices that automatically go into a power standby mode ("sleep") may have expired session tokens that fail when the device attempts to resume connectivity. At the server, failover communications or handshake negotiations with one server may not translate to other clustered servers. Sessions may have to be restarted.

Presentation layer conflicts are often related to changes in encryption keys or updates to service architectures that are not supported by various client devices. For example, an older browser may not interoperate with a script or a new encoding standard.

Application layer network connectivity problems are extremely common. Many applications may conflict with other apps. Apps also may have caching or corrupted files that can be remedied only by uninstalling and reinstalling or by updating to a newer version. Some apps also require persistent connections to updater services or third parties, and network security settings may prevent those connections from being made.

Other troubleshooting steps may include searching log files for anomalies and significant events, verifying that certificates or proper authentication protocols are installed and available, verifying encryption settings, clearing application caches, updating applications, and, for endpoints, removing and reinstalling an application. Search vendor-supported support sites and forums and frequently asked questions (FAQ) pages before you make changes to installed services. You also must be aware of any service-level agreements (SLAs) that your organization must meet.

Always follow proper troubleshooting steps, keep accurate records of any changes that you attempt, document your changes, and publish any remedies so that others can learn from your troubleshooting activities.

Palo Alto Networks Cybersecurity Academy