121. What is System Center 2012 Operations Manager? What are the features and enhancements in Operations Manager 2012?

Ans.:

- Operations Manager enables you to monitor hardware, virtual machines, operating systems, services, applications, devices, and operations for the systems in a computing environment.
- Operations Manager can be used to monitor environments for businesses both large and small, in data center environments, and for private, public, or hosted cloud solutions.
- The new version of Operation Manager 2012 includes a number of new features and incremental improvements.
- These improvements includes the following:

➢ **Enhanced network monitoring:**

- Operations Manager 2012 now can discover and monitor network switches and routers, discovering interfaces and ports on those devices.
- It will even discover virtual Local Area Network (LAN) information.

➢ **Application monitoring:**

- Application monitoring is based on the AVIcode product and allows the monitoring of Internet Server (IIS) hosted .NET applications.
- This is implemented as an easy-to-use monitoring template named .NET Application Performance Monitoring, similar to the Web Application Transaction Monitoring template.

➢ **Resource pools:**

- Resource pools take the place of clustering, allowing the administrator to group Operations Manager objects such as management servers into fault-tolerant pools.
- This eliminates the need for a Root Management server (RMS) server and, more important, an RMS cluster.
- Resource pools allow for easy fault-tolerance to be created within the management group.

➢ **Enhanced Dashboard views:**

- Dashboard views allow for greater customization and flexibility. Rather than being based on other console views, the new dashboards are based on widgets.
- There are three types of widgets: the state widgets, performance widget, and alert widget.

- **SharePoint web part:**

- OpsMgr 2012 provides the SharePoint web part to integrate into SharePoint 2010.
- With this web part, any dashboard you create can be included in a SharePoint website.
- This allows operations data to be Included within other SharePoint portals, providing both detailed and summary information.

- **Orchestrator replaces connectors:**

- In OpsMgr 2007, connectors provided the integration with other consoles and trouble ticket systems.
- However, they had limited programmability and customizable features via the notification process.
- In OpsMgr 2012, Orchestrator 2012 will allow for sophisticated customizations and complex workflows when forwarding alerts and creating trouble tickets.

- **New PowerShell 2.0 cmdlets:**

- OpsMgr 2012 provides a number of new PowerShell 2.0 cmdlets for working with agents, alerts, and management packs.
- All the cmdlets have been renamed and now include a System Center Operations Manager (SCOM) prefix, for example, Get - SCOMAgent rather than Get Agent. There are also a whole new set of cmdlets for Linux and UNIX systems.

- **Improved UNIX and Linux monitoring:**

- OpsMgr 2012 can use unprivileged accounts with the sudo feature rather than require the root password to UNIX and Linux system.
- The UNIX and Linux systems now participate fully in Resource Pools, allowing them to failover to other management servers should their primary fail.

122. What is the functionality provided by Operations Manager 2012? (Or Explain real time monitoring with operations manager 2012.)
Ans.:

- OpsMgr provides various functionalities:

- **Management packs:**

- Application-specific monitoring rules are provided within individual files called management packs.

- For example, Microsoft provides management packs for Windows Server systems, Exchange Server, SQL Server, SharePoint, DNS, and DHCP, along with many other Microsoft technologies.
- Management packs are loaded with the intelligence and information necessary to properly troubleshoot and identify problems.
- The rules are dynamically applied to agents based on a custom discovery process provided within the management pack.

➢ **Monitors:**

- Management packs contain monitors, which allow for advanced state based monitoring and aggregated health rollup of services.
- There are monitors for events, performance, logs, services, and even processes. Monitors also provide self-tuning performance threshold monitoring based on a two- or three-state configuration.

➢ **Rules:**

- Management pack rules can monitor for specific event log data, collect performance data, or even run scripts on a timed basis.
- This is one of the key methods of responding to conditions within the environment. Management pack rules can monitor for specific performance counters.
- This data is used for alerting based on thresholds or archived for trending and capacity planning.

➢ **Alerting and notification:**

- OpsMgr provides advanced alerting functionality such as alert notifications via email, paging, Short Message Service (SMS), and instant messaging (IM).
- Alerts are highly customizable, with the ability to define alert rules for all monitored components.

➢ **End-to-end service monitoring:**

- OpsMgr provides service-oriented monitoring based on System Definition Model (SDM) technologies.
- This includes advanced object discovery and hierarchical monitoring of systems, as well as synthetic transactions that confirm the health of the system from a client perspective.

- This includes URLs, ports, Active Directory, LDAP, database access, and Exchange services.

123. Explain the architectural components of Operations Manager 2012.
Ans.:

- OpsMgr is primarily composed of five basic components: the operations database, reporting database, management server, management agent and operations console.
- The following list describes the different OpsMgr component:-
  - Agents
  - Management Server
  - Operations Manager Database
  - Reporting Data Warehouse
  - Reporting Server
  - Operations Console
  - Web Console
  - Command Shell
  - Gateway
  - Audit forwarder
  - Audit collector
  - Audit collection database
  - Audit Collection Service reporting
- The Operations Manager 2012 architecture is shown in figure with all major component and their data paths.

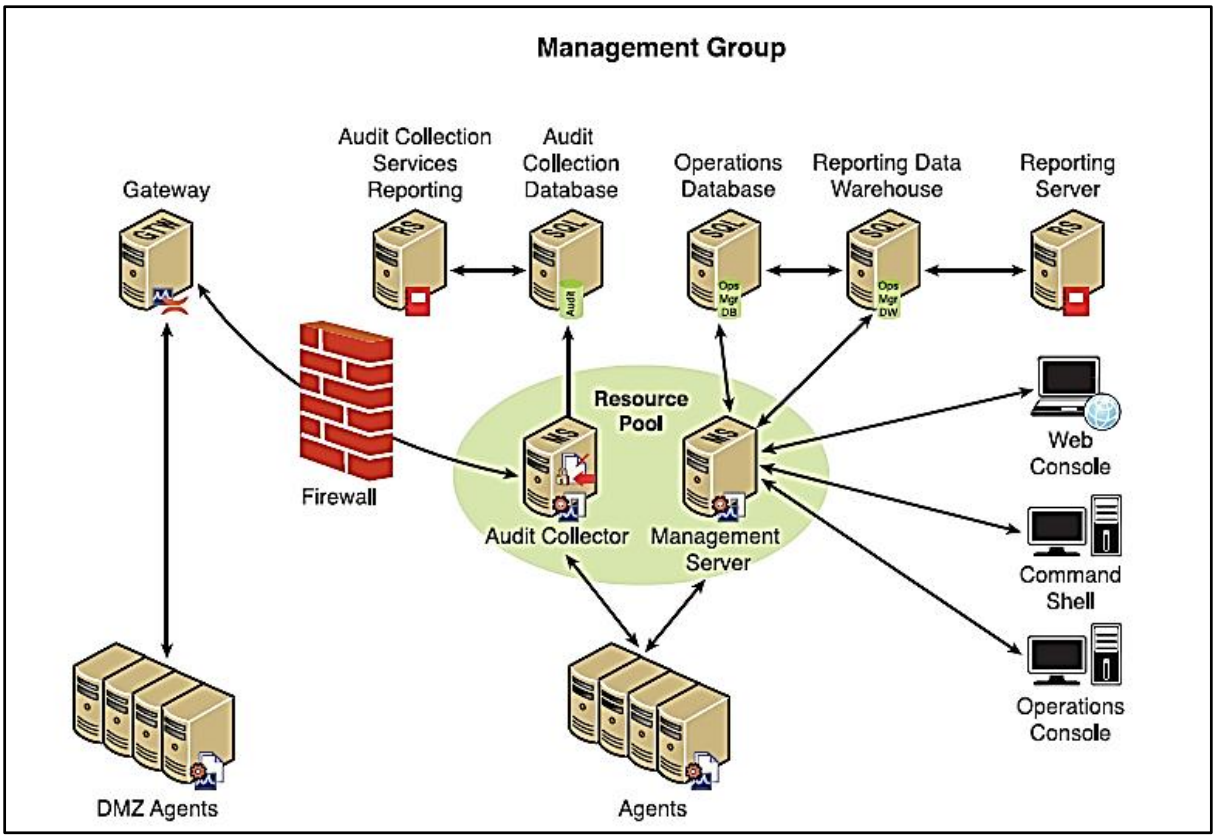

Fig: Operation Manager 2012 Architecture

Agents:-

- Agents are installed on each managed system to provide efficient monitoring of local components.
- The communication is initiated from the agents with the exception of actual agent installation and specific task run from the Operational Console.
- Agents can report to more than one management group at the same time by using multi-homing, allowing for different administration and bifurcation of operations.

Management Server:-

- Management servers can be added for redundancy and scalability. Agents communicate with Management Server to deliver operational data and pull down new monitoring rules.
- Management server also supports agentless monitoring of managed systems and it provides support for audit collection.
- Management server in OpsMgr2012 directly writes to the Operations Database and data warehouse, which eliminates the need to transfer from one database to another.

- Each management server runs Software Development Kit (SDK) and Configuration service and is responsible for handling console communication, calculating health of the environment, and determining what rules should be applied to each agents.

Operations Manager Database:-

- The operation database stores the monitoring rules and the active data collected from monitored system. This database has 7 day default retention period.
- The Operations Database is a Microsoft SQL Server 2008 database that contains all of the data needed by Operations Manager for day- to-day monitoring.
- The most critical resource used by the Operation Manager database is IO-subsystem, but the CPU and RAM are also important.
- OpsMgr operates through a principle of centralized, rather than distributed, collection of data. All event logs, performance counters, and alerts are sent to a single, centralized database, and there can subsequently be only a single operations database per management group.
- The use of a backup and high availability strategy for the OpsMgr database is, therefore, highly recommended to protect it from outage.

Reporting Data warehouse:-

- The reporting database store archived data for reporting purpose. This database has 400 day default retention period.
- Operations Manager 2012 uses Microsoft SQL Server Reporting Services 2008 (SRS 2008) for its reporting engine. SRS provides many enhancements to previous reporting solutions, including easier authoring and publishing.
- Operations Manager 2012 includes an easy to-use graphical report designer as part of the Operations Manager 2012 console.
- As with the Operations Manager database, the most critical resource on the Reporting data warehouse is the I/O subsystem.

Reporting Server:-

- The reporting server component is installed on Reporting Service instance and provides the extensions needed for Operational Manger Report.

- The reports are generated from the Reporting data warehouse and can be generated ad hoc, exported or scheduled for email delivery.
- The reports can be accessed via the Operations Console and security is integrated with the Operations Manager roles.

Operations Console:-

- The operations console is used to monitor systems, run tasks, configure environmental settings, set author rules, subscribe to alerts, and generate and subscribe to reports.
- The consoles automatically scopes to the objects that an operator is authorized to manage in his or her user role.
- This allows the OpsMgr administrator to grant application owners full operator privileges to the Operations Console, but to a restricted set of objects.
- These restrictions are based on Active Directory security principles and are respected by all consoles, APIs, and command shell.

Web Console:-

- The Web console is optional component used to monitor systems, run tasks, and manage Maintenance mode from the web browser.
- The Web console is similar to the Monitoring space in the Operations console, but the Web console has only 24-hour view of performance data.
- The Web console is an excellent choice for application administrators who need console access to the Operations Manager infrastructure, but don't want to go through the trouble of installing the full console.

Command Shell:-

- This optional component is built On PowerShell and provides full command-line management Of the OpsMgr environment.
- A wide array Of PowerShell cmdlets are available that allow for viewing configuration and operations data, as well as setting operational parameters.

Gateway:-

- This optional component provides mutual authentication through certificates for non-trusted systems in remote domains or workgroups.

- The Gateway server is designed to improve management of devices in demilitarized zones (DMZs) or behind firewalls.
- The Gateway server aggregates communication from agents and forwards them to a management server inside the firewall.
- The Gateway server does not have direct access to the database, data warehouse, or Root Management Server.
- The most important resource on a Gateway server is the CPU; however, Gateway servers do not typically require high-end hardware.

Audit Forwarder:-

- Audit Collection Services (ACS) is an optional component used to collect security events from managed systems; this component is composed of a forwarder on the agent that sends all security events, a collector on the management server that receives events from managed systems, and a special database used to store the collected security data for auditing, reporting, and forensic analysis.
- ACS is a service that gathers Windows security log entries in real time and consolidates them in a database for easy access by security auditors.
- The audit forwarder component resides on the managed computer. In Windows clients, the audit forwarder is a component of the agent and is disabled by default.
- In UNIX/Linux clients, the audit forwarder is a separately deployed agent. The agent collects security events from the local security events log and forwards them to the audit collector.

Audit Collector:-

- The audit collector is a management server with the audit collector feature installed on it.
- This component receives security event data from the audit forwarders and inserts the data into the audit collection database.
- The most important resource on an audit collection is the CPU; however, audit collection servers do not typically require high-end hardware.

Audit Collector Database:-

- The audit database is a SQL Server 2005/2008 database (OperationsManagerAC) and has similar requirements to the operations database and reporting database. The most critical resource used by the

audit database is the I/O subsystem, but the CPU and RAM are also important.

- The database handles a large number of operations due to the volume of security events collected.
- In addition, the database conducts daily maintenance at 2:00 a.m. every morning, which places an additional load on the server.
- The edition of SQL is an important factor in the maintenance; in SQL Server Standard Edition, the database is paused and in SQL Server Enterprise Edition, the database continues to accept data.

Audit Collection Service Reporting:-

- The ACS reporting component is installed separately from ACS and consists primarily of a reporting model and set of reports based on the audit collection database.
- These reports provide summaries and analysis of the security events that have been collected.
- The ACS reporting component can be hosted on a separate server, the audit collection database server, Reporting data warehouse, or even the Reporting Server component.
- The security is fully integrated with the OpsMgr Reporting Services security module.

124. How can we secure operations manager 2012? Explain.

Ans.:

Role-based Security Model:-

The Operations Manager infrastructure supports a role-based security model, which allows roles to be defined as profiles and assigned to Active Directory security principles.

There are seven different roles provide a range of authorization options.

- Administrator
- Operator
- Advanced Operator
- Read-Only Operator
- Report Operator
- Author
- Report Security Administrator

Securing OpsMgr Agent:-

Each server that contains an OpsMgr agent and forwards events to management servers has specific security requirements.

All traffic between OpsMgr components, such as the agents, management servers, and database, is encrypted automatically for security, so the traffic is inherently secured.

OpsMgr uses mutual authentication between agents and management servers. This means that the agent and management server must trust a common certificate authority, a simple requirement when the agents reside in the same forest as the management server.

If the agent is located in a different forest or workgroup, client certificates can be used to establish mutual authentication.

If an entire non-trusted domain must be monitored, the Gateway server can be installed in the nontrusted domain, agents can establish mutual authentication to the Gateway server, and certificates en the Gateway and management server are used to establish mutual authentication.

Understanding Firewall Requirement:-

The default port for OpsMgr communications, port 5723, must specifically be opened on a firewall to allow OpsMgr to communicate across it.

The firewall port for the agents is the port that needs to be opened most often, which is only port 5723 from the agent to the management sewers for monitoring. Other ports, such as 51909 for ACS, are more rarely needed.

Action and RunAs Account Security:-

The security of OpsMgr environment can be strengthened by the addition of multiple service account and RunAs account to handle different OpsMgr components and management packs.

The Management Server Account and SDk/ Configuration service account should be configured to use separate credentials, to provide for extra layer of protection in the events that one account is compromised.

Various management packs have their own RunAs account, such as Active Directory management packs and the Exchange management packs.

Securing DMZ Server with Certificates:-

Servers in an organization’s DMZ are usually not domain members and, thus, cannot do automatic mutual authentication with the OpsMgr sewer.

However, these servers are the most exposed in the organization and, thus, a critical asset to be monitored.
There is a well-defined process for using certificates to handle the mutual authentication.
Certificates on both the management servers and the agents are used to mutually authenticate their communications.
The certificates used for mutual authentication must:

- Have the Name field match the computer name in the Computer Properties
- Be configured with Server (1.3.6.1.5.5.7.3.1) and Client (1.3.6.1.5.5.7.3.2) OIDs
- Be marked as Exportable
- Have their issuing CA trusted by the computer

125. What is fault tolerance and disaster recovery? How is this achieved in operations manager 2012?
Ans.:
Refer Pg No. 230