سرفصل آموزشی

پک حرفه‌ای مهندسی شبکه

فهرست سرفصل‌های دوره‌های آموزشی

سرفصل‌های دوره آموزشی

Zabbix

Zabbix Introduction

Monitoring Concept

- What is Monitoring?
- Monitoring Types
- Monitoring Best Practices
- Define a sample Telecom service flow

Introduction to Zabbix

- What is Zabbix?
- Zabbix functionality
- Usage of ZABBIX in DevOps and ITIL
- Architectures

Introduction to Zabbix components

- Zabbix Server
- Zabbix Proxy

- Zabbix Agent
- Zabbix Web Frontend

Methods of Zabbix Deployments

- Stand Alone
- Distributed
- Multi Branch

Metric collection Methods

- Agent Based
- Agent Less

Problem Detection

- Trigger and Threshold Definition
- Forecasting
- Notifications and Escalation

Installation

Component to install

- Zabbix Server: Version 7.0 LTS
- Database: MariaDB 11
- Zabbix Front End: Apache web server & PHP 8

Installation Methods

- Install using pre-compiled packages
- Install Zabbix Server using Docker images
- Compile Zabbix Server from source

OS Preparation (Rocky Linux 9 - Minimal)

- Install necessary initial packages
- Network settings
- Time settings
- Install Zabbix Agent

Security settings

- Firewall
- Creating SELinux policies for Zabbix

Quick Start

- Prepare a Target Host
- Adding first host in Zabbix
- Adding first item in Zabbix
- Adding first trigger in Zabbix
- Receiving problem notification

Getting Started

- Host Group Configuration
- Host Configuration
- Host name
- Templates
- Host Interface:
- Agent
- SNMP
- IPMI
- JMX
-

Host user custom macros

Inventory

- Item Configuration

  - Item keys
  - Item intervals
  - Simple intervals
  - Custom intervals
  - Flexible
  - Scheduled
  - Item retention time
  - History retention
  - Trend retention
  - Value mapping

- Item types

  - Simple Check
  - ICMP check
  - TCP port

Scenario

- check ping and a TCP port availability of target server
- SSH Agent

Scenarios

- Configure Zabbix server/proxy to use SSH agent
- Check status of an application in target server using SSH
- Telnet Agent

Scenarios

- Configure Zabbix server/proxy to use Telnet agent
- Check status of an application in target server using Telnet
    - Zabbix Agent
    - Zabbix agent vs Zabbix agent 2
    - Active Zabbix agent
    - Passive Zabbix agent
    - Zabbix agent default keys and functions
    - Zabbix agent configuration file
    - Define agent custom function using “Alias” directive
    - Define agent custom function using “UserParameter” directive
    - Restrict Zabbix agent functionality

Scenarios

- Install Zabbix Agent 2
- Change configuration of Zabbix agent

- Add Items using Zabbix agent default functions:
    - Check agent availability
    - Check host uptime
    - Check network interfaces bandwidths
    - Check disk space availability
    - Export some monitoring data from text file
    - Check status of an application on target server
- Configure Zabbix agent file to allow Zabbix server run remote commands
- Check status of an application on target server using remote commands
- Add an "Alias" to check status of an application on target server
- Add an "UserParameter" to check status of an application on target server
- Log monitoring using Active check

SNMP Agent

What is SNMP?

- OID
- MIB

SNMP Versions

- SNMP v1
- SNMP v2
- SNMP v3

Data collection methods

- Get
- Walk

Scenarios

- Configure SNMP server
- Add Items to monitor server using SNMP agent:
  - Check host uptime
  - Check network interfaces bandwidths
- Add SNMP Walk Item
- Import custom MIB file to server
  - External Check
  - Enabling External Scripts

Scenarios

- Writing script and create ExternalCheck item
- Zabbix Trapper
- Sending item value to Zabbix using trapper

Scenarios

- Install Zabbix Sender
- Writing script to get value and send to Zabbix server

Web Scenario Monitoring

- Monitoring Websites and Webservices status, speed, size

Scenarios

- Monitor example website
- Monitor chained web scenario with login and logout steps

HTTP Agent

- Retrieving data from web services, APIs, HTTP endpoints

Scenarios

- Monitor NGINX status using http agent
- Get and monitor weather data from openweathermap

Dependent Item

- Optimizing Metric Collection
- Gathering Multiple Metrics Simultaneously
- Working with Item Pre-Processing

Scenarios

- Get multiple OIDs with SNMP Walk in one item and put them in multiple dependent items
- Get JSON data from an API in one item and put them in multiple dependent items
- Explain and test all pre-processing functions such as:
    - Regular expression
    - XML XPath
    - JSON Path

  - CSV to JSON
  - Custom multiplier
  - Simple change
  - Change per second
  - Discard unchanged

ODBC Monitoring

- Database monitor item type using SQL queries
- Integration to RDBMS databases using UnixODBC
  - Install drivers for databases
  - Definition of DSN (Data Source Name)
  - Creating Item to get single value or multiple values as JSON
  - Tuning of SQL queries

Scenarios

- Install and configure MariaDB/MySQL ODBC driver
- Integration of Zabbix and ODBC
- Monitoring E-Shop payment status by SQL

Calculated Items

- Calculate item values using various functions (Aggregation, Mathematical, …)
- Calculate dynamically for discovered items
- Forecasting item values

Scenarios

- Calculate Success rate
- How to manage division by zero
- Forecasting value based on history

Triggers

- Configuring and creating a trigger
    - Define and tune Thresholds to prevent
- Trigger expression
    - Define Problem and Recovery Expressions
    - Functions
    - Aggregate functions
    - Bitwise functions
    - Date and time functions
    - History functions
    - Trend functions
    - Mathematical functions
    - Operator functions
    - Prediction functions
    - String functions
- Operators
    - Comparison between some items
    - Mathematical Operator
    - Logical Operator (And, Or)

Scenarios

- Create various triggers
    - Trigger dependencies
    - Trigger and Event Correlations

    - Predictive trigger functions

Templates

- Using Templates
- Find and import third party templates
- Create a Template
- Export Templates

Discoveries

- Network Discovery
    - Top-Down Discovery
    - Finding Network Devices using various criteria
- Auto Registration
    - Bottom-Up Discovery
    - Configuring Active Zabbix Agent to Auto Register device to Zabbix
- Low Level Discovery (LLD)
    - Finding Low Level Metrics using following methods:
    - Zabbix Agent
    - External Script
    - Trapper
    - SNMP
    - HTTP Agent
    - ODBC
    - Create Item prototype
    - Create Trigger prototype
    - Configure Trigger prototype thresholds dynamically

Scenarios

- Creating Low Level Discovery rule based on E-Shop Payments (ODBC)
- Creating Low Level Discovery rule based on SNMP and SNMP Walk
- Creating Low Level Discovery rule based on External Script

Zabbix Proxy

- Zabbix Proxy
    - Active Zabbix Proxy
    - Passive Zabbix Proxy
- Zabbix Proxy Load Balancing (Proxy Group)

Securing Zabbix

- Data Transformation Encryption
    - Between Zabbix Agent and Zabbix Proxy
    - Between Zabbix Agent and Zabbix Server
    - Between Zabbix Proxy and Zabbix Server
    - Secure Web Frontend using https

User and Group Management

- User
- Group
- Role
- Permissions

Performance Tuning

- Kernel Parameters
- Database Tuning

    - MySQL Partitioning
    - Optimize tables
    - Adding Primary Key to Zabbix Database
    - Configuring Elasticsearch as Storage

Zabbix Deployment

- Install Zabbix Using Docker
- Monitoring Docker with Zabbix Agent2
- Install Zabbix Using Source Code

Zabbix Administration

- Zabbix Server and Proxy Configuration File
- General
- Audit Log
- Housekeeping
- Queues

Reports

- System Information
- Top 100 Triggers
- Inventory Report

Alerts and Notification

- Create and Configure Media types

Scenario

- Adding and configuring Email Media
- Optional: Adding and configuring Telegram (with Graph) Media

Configure Trigger Actions

Configuring Escalation Policy

Configure Maintenance time

Zabbix Visualization

- Creating Zabbix Dashboard
- Using Widget and panels
- Dynamic Widgets
- Slide Show
- Zabbix Map

Optional: Grafana

- Install and Configure Grafana
- Add and integrate Zabbix data source Plugin
- Creating sample dashboard on Grafana

سرفصل‌های دوره آموزشی

Ansible

Introduction of DevOps

Understanding DevOps concepts

DevOps Automation

Continuous Integration

Continues Delivery

Continuous Deployment

The roles of Ansible in CI/CD

The benefit of CICD

What is Ansible?

Automation Deployment Pipeline

Need of Ansible

What Ansible can do?

Advantages of using Ansible?

Agent-Based VS Agentless systems

Ansible’s Agentless Architecture

Install Ansible

Validate Ansible Installation

Ansible Vs Puppet Vs Chef Vs SaltStack

Ansible Architecture

Host, Group and Host Inventory

Ansible Ad-Hoc commands

Playbooks, plays, tasks and modules

Ansible configuration

Ansible-playbook Structure

Taks, vars, files, templates, meta, defaults, handlers

Ansible-playbook Syntax

Run ansible playbook

Variables, variable types and priorities

Command, expect, script, shell and raw modules file, copy and fetch modules

Group and user modules

zyper_repository, zypper, yum_repository and you modules

Template, lineinfile, replace and service module

Archive and unarchive module

Async actions and concurrent tasks

wait_for and wait_for_connection modules

Mail module

Subversion and git modules

get_url, timezone and iptables modules

Mariadb modules

Find module and local_action feature

Conditions

Loops

Standard loops

Nested loops

Import playbooks and tasks

Handlers

Ansible Vault

Encrypt files and strings

Vault ID

Implement an Ansible playBook to Setup a webserver

Integrate Jenkins & Ansible

CICD with Git, Jenkins and Ansible (Application Deployment)

Ansible & VMWare

Ansible & Cisco

Ansible & Mikrotik

Develop Custom Module

Module format

Module’s return value and error handling

Setup nginx servers behind haproxy via Ansible playBook

Ansible & Windows Hosts

Manage windows features

Manage windows services

Execute shell module on windows

Windows Package management

Package Silent Installation

Implement an Ansible PlayBook to Setup IIS

Integrate Ansible and Docker

Docker_image and docker_image modules

docker_container and docker_container modules

docker_network and docker_network_info modules

docker_volume and docker_volume_info modules

docker_swarm module

Ansible Galaxy

Ansible Tower

Ansible AWX

AWX prerequisites and Installation

AWX Dashboard

AWX - organizations, teams and users

AWX - hosts, groups and inventory

AWX - credentials

AWX - projects and templates

AWX - Schedule templates, notification and permissions

سرفصل‌های دوره آموزشی

ELK Stack

Introduction to Elastic Stack

- What is the Elastic Stack? Overview and History
- Working with data, structured vs. semi-structured vs. unstructured data
- Overview of the data analysis process
- What is Big Data? Characteristics (3Vs: Volume, Velocity, Variety)
- Elastic Stack vs. ELK Stack, Evolution and Components
- Common Use Cases: Log Management, Business Analysis, Security Analytics, Monitoring
- Installing Elastic Stack Components: Elasticsearch, Logstash, Kibana, Beats

Deep Dive into Elasticsearch

- Elasticsearch Architecture: Nodes, Clusters, and Indexes
- What is API and advanced usage of API in Elasticsearch
- Data Modeling and Indexing
- Understanding Mapping, Documents, and Fields
- CRUD Operations: Create, Read, Update and Delete data
- Search Queries: Term, Match, Range, Aggregations
- Advanced Search and Filtering: Bool Queries, Nested, and Geo Queries
- Performance Tuning with Sharding, Replication, Caching, and Index Management

Data Collection with Logstash

- Introduction to Logstash, architecture and Pipeline Concepts
- Configuring input plugins for various data sources
- Reading data from different sources (logs, metrics, CSVs, Databases, etc.)
- Input Plugins: File, Syslog, Beats, JDBC
- Data Transformation using filters for parsing, enriching, and transforming data
- Output Plugins: Elasticsearch, File, Email, Kafka
- Managing and Debugging Pipelines
- Logstash Configuration Best Practices

Data Visualization with Kibana

- Introduction to Kibana, Interface and Navigation
- Index Patterns and Data Discovery
- Building Visualizations with Pie Charts, Bar Graphs, Line Graphs, and Maps
- Creating Dashboards for Monitoring and Analytics
- Working with Kibana Lens for Simplified Data Exploration
- Advanced Visualizations: Timelion, Vega, Canvas
- Alerts and Reporting in Kibana
- Alarm and triggers in Kibana
- Security and Access Control in Kibana

Data Shipping with Beats

- Overview of Beats: Filebeat, Metricbeat, Packetbeat, Auditbeat, Heartbeat
- Installing and Configuring Beats
- Collecting and Parsing Log Files with FileBeat
- System and Application Metrics with MetricBeat
- Network Traffic Analysis with PacketBeat
- Security Event and File Integrity Monitoring with AuditBeat
- Uptime Monitoring with HeartBeat

- Sending Data from Beats to Elasticsearch/Logstash

Unified Data Collection with Elastic Agent

- Introduction to Elastic Agent
- Replacing Beats with Elastic Agent
- Configuring Elastic Agent for Data Collection (Log and Metric)
- Centralized Management with Fleet

Security and Monitoring in the Elastic Stack

- Securing the Stack: Role-Based Access Control (RBAC) and Encryption
- HTTPS interfaces and Secure communications
- Auditing and Compliance, Monitoring Access and Changes
- Implementing Security Rules and Alerts
- SIEM (Security Information and Event Management) and SOC Use Cases

Advanced Elastic Stack Topics

- Machine Learning in Elastic Stack: Anomaly Detection and Forecasting
- IoT integration with Elastic Stack
- Advanced alarm and triggers deployment (sending email, SMS, Physical action, etc)
- APM (Application Performance Monitoring): Tracing and Performance Metrics
- Scaling Elasticsearch Clusters, High Availability and Load Balancing
- Backup and restore Strategies for Elasticsearch
- Handling Large Datasets, Index Lifecycle Management (ILM) and Rollups

Real-World Use Cases and Projects

- Setting Up a Centralized Logging Solution
- Building a Real-Time Monitoring Dashboard for Infrastructure Metrics
- Security Analytics and Threat Detection with the Elastic Stack
- Implementing Application Performance Monitoring (APM) for services
- IoT Management and monitoring platform with elastic stack