سرفصل آموزشی

# پک حرفه‌ای متخصص امنیت

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 multi-

ple 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

# Prometheus

## Overview

- What is DevOps?
- What is Monitoring?
- What Is Prometheus?
- Prometheus Architecture

## Getting Started with Prometheus

- Running Prometheus
- Using the Expression Browser
- Running the Node Exporter
- Alerting

## Instrumentation

- A Simple Program
- The Counter
- Counting Size
- The Gauge
- The Summary
- The Histogram

- Unit Testing Instrumentation
- Approaching Instrumentation

## Exposition

- Python
- Go
- Java
- Pushgateway
- Bridges
- Parsers
- Exposition Format

## Labels

- Instrumentation and Target Labels
- Aggregating
- Label Patterns

## Dashboarding with Grafana

- Grafana Installation
- Data Source
- Dashboards and Panels
- Graph Panel
- Singlestat Panel
- Table Panel
- Template Variables



## Node Exporter

- CPU Collector
- Filesystem Collector
- Diskstats Collector
- Netdev Collector
- Meminfo Collector
- Hwmon Collector
- Stat Collector
- Uname Collector
- Loadavg Collector
- Textfile Collector

## Service Discovery

- Service Discovery Mechanisms
- Relabelling
- How to Scrape

## Containers and Kubernetes

- cAdvisor
- Kubernetes
- Common Exporters:
- Consul
- HAProxy
- Grok Exporter
- Blackbox

## Working with Other Monitoring Systems

- Other Monitoring Systems
- InfluxDB (TICK Stack)
- Zabbix

## Writing Exporters

- Consul Telemetry
- Custom Collectors
- Guidelines

## Introduction to PromQL

- Aggregation Basics
- Selectors
- HTTP API

## Aggregation Operators

- Grouping
- Operators
- Binary Operators
- Working with Scalars
- Vector Matching
- One-to-One
- Many-to-One and group_left
- Many-to-Many and Logical Operators
- Operator Precedence

## Functions

- Changing Type
- Math
- Time and Date
- Labels
- Missing Series and absent
- Sorting with sort and sort_desc
- Histograms with histogram_quantile
- Counters
- Changing Gauges
- Aggregation over Time

## Recording Rules

- Using Recording Rules
- When to Use Recording Rules
- Naming of Recording Rules
- Alerting:
- Alerting Rules
- Configuring Alertmanagers

## Alertmanager

- Notification Pipeline
- Configuration File
- Alertmanager Web Interface

## Putting It All Together

- Planning a Rollout
- Going Global with Federation
- Long-Term Storage
- Running Prometheus
- Hardware
- Configuration Management
- Networks and Authentication
- Planning for Failure
- Managing Performance
- Managing Change
- Getting Help

سرفصل‌های دوره آموزشی

# Python

**Introduction:**

- Python History
- Python Features & usage
- Python versions & differences
- Interactive Environment and Interpreter of Python
- Python IDEs and PyCharm
- Running Python files from Terminal & IDE by example
- PyCharm Environment & Debuging with PyCharm

**Python program structure:**

- Storing code and running program
- Variables and Datatypes
- Naming rules & conventions
- Getting user input and displaying output to terminal
- Introduction to Object Oriented programming & Objects in Python
- Modularity & Python libraries
- Installing & using libraries in python

## Computational Operators:

- Logical Operators
- Operator priority
- Exceptions & Exception Handling in Python
- Basic DataTypes & Literals
- Lists, Tuples, Sets, Sequences and dictionaries
- List & Tuple Methods Slicing And Concatenation of Sequences
- Dictionary methods
- List Comprehensions

## Strings and coding:

- Unicode
- Excape Characters
- Multiline Strings
- Type casting in python
- String Methods
- String formatting

## Conditional statements:

- Loops
- For loop
- While loop
- Loop controlling statements
- Nested Loops
- Using loops on Sequences & dictionaries

## Working with files:

- Binary & Text files
- File Opening modes
- Working with file offset pointer
- Bytes and bytearrays
- With statement
- Working with csv files

## Functions in python:

- Function definition structure
- Documenting objects in python and self documented concept
- Calling functions variable scope in functions (global, local , nonlocal)
- Optional function parameters
- Lambda functions

## Libraries in python:

- Library Structure & Creating Libraries
- Separating program logic from helping entities
- Frequent libraries & their usage
- Sys library
- Getting script parameter from terminal
- Os library
- Working with OS directory structures using os library



## Regular Expressions:

- Re library
- Urllib & request libraries
- Web scraping using urllib, request & re libraries

## Class definition:

- Class initiation
- Inheritance
- Class methods and variables
- Example of using classes versus functional programming