==========

-: OKTA ADMIN COURSE RUNNING NOTES :-

==========

01) Identity Manager (IDM) basic Architecture and it's usage.
02) Access Management(AM) basic Architecture and it's usage.
03) What is Single Sign On (SSO)? Advantages of using SSO.

Single sign-on (SSO) in the enterprise refers to the ability for employees to log in just one time with one set of credentials to get access to all corporate apps, websites, and data for which they have permission. SSO solves key problems for the business by providing:

- Greater security and compliance.
- Improved usability and employee satisfaction.
- Lower IT costs.

04) Identity and Access Management (IDAM/IAM) Terminology.
- Doc Shared

05) Different IDAM competitors available in the market.

IDM : OIM, SailPoint, QOIM, Saviynt, IBM Tivoli etc..
AM : OAM, SiteMinder, Okta, ForgeRock, Ping Federation etc..

06) Overview on Cloud vs On-Premises Applications/Tools.

Essentially, the fundamental difference between cloud vs on-premise software is where it resides. On-premise software is installed locally, on your business' computers and servers, where cloud software is hosted on the vendor's server and accessed via a web browser.

Cloud software advantages
- Anywhere and anytime access
- Affordable
- Predictable costs
- Worry-free IT
- High levels of security
- Quick deployment
- Scalability
- Lower energy costs

07) What is Okta ? and why Okta?

OKTA is a cloud based identity and access mananagement solution that provides authentication, authorization, multi-factor authentication, and user lifecycle management services. In addition, it provides enterprise single sign-on authentication experience to employees, contractors, and agents for web-based applications.

https://www.okta.com/resources/whitepaper/okta-security-technical-white-paper/
A white paper in the tech industry is a technical document that describes how a technology or product solves a particular problem.

https://status.okta.com/
https://trust.okta.com/

08) Okta Terminology.
- Doc Shared

09) Okta developer account creation and Admin Dashboard overview.

https://www.okta.com/free-trial/ (Work Force Identity - Business email required)
https://www.okta.com/free-trial/customer-identity/ (Customer Identity - gmail suffice)
https://developer.okta.com/signup/ (Okta Developers Sign Up - gmail is suffice)

10) Types of users in Okta.

Three Types of People in Okta :

Okta-sourced : Profile managed by Okta, Authenticated by Okta, Credential store :(Yes) Okta
Directory-sourced : Profile managed by Directory, Authenticated by Directory/Delegated Authentication, Credential store : (Yes) LDAP
Application-sourced : Profile managed by Application, Authenticated by Directory or Okta, Credential store : No

- End Users :- End users are people who use Okta to access applications (who leverage Okta services)
- Administrators :- Admin are Okta administrators who use Okta to administer their org (who manages Okta)

11) Ways to create users in Okta.

- Local user creation via Admin Portal (Directory >> People >> Add Person)
- Via .csv file (limitation : 10 MB, 10000 users)
- From Postman or any Coding (By using API Calls)
- Import from Directories (like AD and LDAP) and Target applications (like Box, SalesForce etc)

Okta mandatory Attributes:
- login (Username) - We can't make it as Optional
- firstName (First Name) - We can make it as Optional
- lastName (Last Name) - We can make it as Optional
- email (Email) - We can't make it as Optional

12) Different User Statuses in Okta.

- Active :- The user account is active and the person can access all assigned applications.
- Password Expired :- The account password has expired and needs to be changed.
- Password Reset :- The user is allowed to resolve forgotten password issue by resetting the password without relying on the service desk.
- Pending User Action :- The user account has been added and the activation has been initiated, but the user has not yet set a password.
- Locked Out :- The account has been locked due to a consecutive number of incorrect passwords used.
- Suspended :- The user cannot log in due to an action taken by an administrator.
- Deactivated :- The user account is inactive and admin can’t assign any applications to the user.
- Staged :- The (new) user account has been

created, but the activation process has not been initiated.

- Delete :- User account permanantly Deleted from Okta (We cannot see this status in Okta)

13) Okta Lifecycle management Operations.

- CRUD (Create, Read, Update, Deactivated/Delete/Disable, Activate)

14) Understanding Okta Universal Directory.

Universal Directory allows you to store employee, partner, and customer profiles in Okta, generating a user-based, single source of truth.

(OR)

One place to manage all your users, groups and devices. That's what Universal Directory offers: huge time and effort savings. For a business world increasingly concerned with authentication and identity management, the tool offers a transformative approach to cumbersome directory challenges.

15) Okta Groups and Group Operations.

A Group is basically an assemblage of people. It can be understood as a collection of individuals (two or more). These are the foundation of an organization.

Group Operations :

- Create Group
- Add Users to the Group (Diff ways to add users into Group)
- Remove Users from the Group (Diff ways to add users into Group)
- Delete Group

Three Types of Groups available in Okta :

1) Okta Groups : • Okta groups are created and membership is managed in Okta.
• Only Okta groups can contain Okta, directory and application sourced users.

2) Directory Groups : • Directory groups are created and membership is managed in the external directory service.
• Only directory-sourced users can be members of directory groups; this is established in the external directory service.
• Directory groups are copied into Okta.
• If the external directory instance is deactivated or deleted, the associated groups no longer appear in Okta.

3) Application Groups : • Application groups are created and membership is managed in the application.
• Members of application groups are pulled into Okta during application creation.
• Application groups are copied into Okta.
• If the application connector is deactivated or deleted, the group no longer appears in Okta.

16) Okta API Tokens (Token creation and verify validity of a token)

API (Application Programming Interface) is something that allows one piece of software to talk to another piece of software.

There are lots of diff kinds of API's but when you hear people talk about Okta's API or Google's API etc.. what they are talking about is a REST API. REST stands for Representational State Transfer.

REST API works pretty much the same way a website does. You make a call from client to a server and you get data back over the http protocol.

API tokens are used to authenticate requests to the Okta API just like HTTP cookies authenticate requests to the Okta Application with your browser. An API token is issued for a specific user and all requests with the token act on behalf of the user. API tokens are secrets and should be treated like passwords.

When you use an application on your mobile phone, the application connects to the Internet and sends data to a server. The server then retrieves that data, interprets it, performs the necessary actions and sends it back to your phone. The application then interprets that data and presents you with the information you wanted in a readable way. This is what an API is - all of this happens via API.

To explain this better, let us take a familiar example.

Imagine you're sitting at a table in a restaurant with a menu of choices to order from. The kitchen is the part of the "system" that will prepare your order. What is missing is the critical link to communicate your order to the kitchen and deliver your food back to your table. That's where the waiter or API comes in. The waiter is the messenger – or API – that takes your request or order and tells the kitchen – the system – what to do. Then the waiter delivers the response back to you; in this case, it is the food.

00uQ6LGCZ7vyOYCXSZjvj6Ai__DAc9yu4UDpF9n0bL - Default validity of an API Token : 30 days

Sample API Calls:
To get All Okta users -
https://dev-63389365.okta.com/api/v1/users/
To get current user Okta Session -
https://dev-63389365.okta.com/api/v1/sessions/me

17) Postman Introduction, Setup and it's usage.

Postman is a collaboration platform for API development. Postman's features simplify each step of building an API and streamline collaboration so you can create better APIs—faster.

(OR)

Postman is an API(application programming interface) development tool which helps to build, test and modify APIs. It has the ability to make various types of HTTP requests(GET, POST, PUT, DELETE), saving environments for later use, converting the API to code for various languages(like JavaScript, Python, .net etc..).

Immutable ID : value that cannot be changed as long as the object it refers to exists. it's unique for each object(User or Application or Group)

For Users it's start with 00uxxxxxx (Eg : 00uno3xm6RMbDYiNd5d6)
For Groups it's start with 00gxxxxxx (Eg : 00gno3xm6RMbDYiNd5d6)
For Applications it's start with 00axxxxxx (Eg : 00ano3xm6RMbDYiNd5d6)

Link to Download Postman Software : https://www.postman.com/downloads/
Link to import Okta API collections into Postman : https://developer.okta.com/docs/reference/postman-collections/

Postman Methods for Okta APIs:

GET – To read/get info from Okta
POST – To add new data into Okta
PUT – To replace/update existing data in Okta
DEL – To delete existing data in Okta

HTTP response status codes

Informational responses (100 – 199)
Successful responses (200 – 299)
Redirects (300 – 399)
Client errors (400 – 499)
Server errors (500 – 599)

18) Rockstar setup and it's usage.

Add rockstar extension to your Chrome browser to export user/group/app details from Okta to your local machine.

19) Connect Okta with Python code.

- Download and install Python Software in your machine
- Write code as per business requirement (Call required API calls and configute Okta tenant details like Okta Org URL and API Token)
- Execute it

20) Perform bulk operations using Postman.

- Create a csv file and add the header(variablename in the first row and first column).
- Add userids (immutable ids) from second row onwards
- Save the file in your computer.
- Open Runner tool in your postman, select your environment, upload your .csv file (which you saved in above step) and drag & drop required operations (Eg:Deactivate, Activate, Delete etc..) that you want to perform then click on Start Run

21) Okta Administrators (Individual vs Group based admin access).

- Super Admin
  Perform all admin activities for an org. Super admins have full management access.

- Organization Admin
  Perform most admin activities for an org. Note: Org admins cannot manage applications, authorization servers, hooks, Okta Mobile, or other admins.

- Group Admin
  Manage users, their profiles, and their credentials. Note: You can specify one or more groups after selecting this role.

- Application Admin
  View and manage user permissions in an application. Note: You can specify one or more applications after selecting this role.

- Read-Only Admin
  View most data in the Admin Console.

- Mobile Admin
  OMM - (EA): Mobile admins can perform actions related to mobile policies, sign-on policies, mobile devices, and Okta Mobile.

- Help Desk Admin
  View and unlock users, reset passwords and reset MFA. Note: You can specify one or more groups after selecting this role.

- Report Admin
  View all reports and the System log.

- API Access Management Admin
  Build custom authorization servers to protect your API endpoints.

- Group Membership Admin
  Manages the membership of groups. Note: You can specify one or more groups after selecting this role.

Link to know the Okta Admin access details : https://help.okta.com/en/prod/Content/Topics/Security/administrators-admin-comparison.htm

22) LDAP Terminology.

What is LDAP?

LDAP - Lightweight Directory Access Protocol

It is a protocol separately designed for accessing the directory services which can store the information of the entire organization into a central repository.

LDAP provides the communication language that applications use to communicate with other directory services servers.

Directory services store the users, passwords, and computer accounts, and share that information with other entities on the network.

Directory Information Tree (DIT)

The directory information tree (DIT) provides a way to refer to the data stored in your directory. The types of information stored, the physical nature of your enterprise.

DIT is data represented in a hierarchical tree-like structure consisting of the Distinguished Names (DNs) of directory service entries

O = Organization
C = Country
OU = Organization Unity
CN = Common Name
SN = Sur Name
DN = Distinguished Name (Complete User/Group address where it stored in the Directory)

Eg : CN=Abc, OU=Hi-Tech, OU=Hyd, OU=India DC=Vodafone, DC=com (bottom to up)

Default port of LDAP : 389

23) Different LDAP Competitors available in the market.

- AD (Active Directory)
- OUD (Oracle Unified Directory)
- OID (Oracle Internet Directory)
- IBM Tivoli Directory Server
- Sun Java System Directory Server
- eDirectory: NetIQ
- OpenLDAP
- Red Hat Directory Server
- and many more

24) Advantages of using LDAP.

- LDAP is mainly used for read operations instead of Write operations
- It's light weight and very faster in terms of data retreval
- Global naming model ensures unique entries.
- It allows use of multiple independent directories.
- It is extensible to meet future/local requirements.
- It runs over TCP/IP and SSL directly.
- It has wider support across the industries.
- The protocol is based on existing deployed technologies.
- LDAP is used by many services like TCP and DNS.
- It is open source protocol with very flexible architecture.
- LDAP is automated and hence updating of the same is much easier unlike DNS.

25) Basic overview of Active Directory and AD operations.

AWS Trail sign up : https://portal.aws.amazon.com/billing/signup#/start

AD Database Name : NTDS.DIT
NTDS stands for NT Directory Services. The DIT stands for Directory Information Tree.

Server Setup and AD installaion and Domain Creation

- Install Windows Server 2012 R2 in your virtual machine or Sign up Amazon Webservice trail version for 12 months free then create Windows Server 2012 R2 instance.

- After server creation, login to the server via RDP
Once login, change the Server hostname for better namng convention. (Server manager >> local server >> Computer Name >> Change >> Change the computer name) then restart the server.

- After Server restart, enable the AD feature (Server manager >> Dashboard >> Add roles and features >> Rolebased or feature based installation >> Active Directory Domain Services)

- Once AD feature is Enabled configure the same (providedomain name and netbios name) then restart the server

Microsoft’s Active Directory (AD) :
AD is the most widely implemented directory service in the world – built many of its underpinnings on LDAP while also extending the concept of directory services with many proprietary extensions. LDAP has most often been used for more technical situations and organizations.

Active Directory is a directory services implementation that provides all sorts of functionality like authentication, group and user management, policy administration and more.

AD does support LDAP, which means it can still be part of your overall access management scheme.

Active Directory is just one example of a directory service that supports LDAP. There are other flavors, too: Red Hat Directory Service, OpenLDAP, Apache Directory Server, and more (Above (Topic 23) are the different LDAP competitors).

Basic AD Operations:
- OU Creation
- User Creation
- Group Creation
- Disable User
- Enable User
- Delete User
- Add User to Group
- Remove user from the group

26) Understanding TLS 1.2 protocol and enabling it in Agent installed servers.

https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information. The two terms are often used interchangeably in the industry although SSL is still widely used. When you buy an 'SSL' certificate from DigiCert, you can of course use it with both SSL and TLS protocols.

TLS 1.2 Path : TLS Full Form - Transport Layer Security

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server] "DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client] "DisabledByDefault"=dword:00000000

27) Different types of Tenants/environments.

- Prod (Production)
- Stage (stg) -Staging
- Tst (Testing)
- UAT (User Acceptance Test)
- Dev (Development)
- Preview Tenants (Lower Environments)

28) Active Directory Integration with Okta (AD Agent Installation and Configuration).

LDAP vs. Active Directory

LDAP is a way of speaking to Active Directory.

LDAP is a protocol that many different directory services and access management solutions can understand.

The relationship between AD and LDAP is much like the relationship between Apache and HTTP:

HTTP is a web protocol.
Apache is a web server that uses the HTTP protocol.
LDAP is a directory services protocol.
Active Directory is a directory server that uses the LDAP protocol.

Occasionally you'll hear someone say, "We don't have Active Directory, but we have LDAP." What they probably mean is that they have another product, such as OpenLDAP, which is an LDAP server.

It's kind of like someone saying "We have HTTP" when they really meant "We have an Apache web server."

- Agent (AD, LDAP, IWA, RADIUS and OPP)

Okta Active Directory Agent: A lightweight agent that can be installed on any Windows Server and is used to connect to on-premises Active Directory for user provisioning, deprovisioning, and authentication requests.

The Okta Active Directory (AD) agent enables you to integrate Okta with your on-premise Active Directory (AD). AD integration provides delegated authentication support, user provisioning and de-provisioning. To enable AD integration, you must install the Okta AD agent, and import AD users and groups into Okta.

29) AD Delegated Authentication.

- Delegated authentication: if you want Active Directory to authenticate your users when they sign in to Okta. A user's Okta credentials are the same as their Active Directory credentials when delegated authentication is on.

30) Okta general terms.

- Early Access (EA) vs General Availability (GA)
- Schema Discovery, Org
- Agent (AD, LDAP, IWA, RADIUS and OPP)

31) Differences between Okta Mastered users/groups, Directory mastered users/groups and Application mastered users/groups.

- We cannot edit user's profile when profile sourcing is enabled, if we want to update user profile we need to update it in AD/LDAP post that same details will be synced to Okta.

- We cannot add/remove users to/from AD mastered groups (which are imported from AD/LDAP) and we cannot delete these groups in Okta. If we want to add/removed users from these groups we need to do that in AD/LDAP.

32) Different types of imports available in Okta.

- Incremental import (fastest)

Only imports Active Directory users that were created or updated since your last import. Users not present in the data will not be changed.

(This is the type of import performed by automatic scheduled imports.)

- Full import (could take a while)
Replaces all user data with the imported user set. Users not present in the data will be deactivated.

33) What is JIT Provisioning?

Just-In-Time (JIT) provisioning enables automatic user account creation in Okta the first time a user authenticates with Active Directory (AD) Delegated Authentication, Desktop SSO, or inbound SAML.

JIT account creation and activation only works for users who are not already Okta users. This means that users who are confirmed on the import results page, regardless of whether or not they were subsequently activated, are not eligible for JIT activation. When JIT is enabled, users do not receive activation emails.

If delegated authentication is enabled, you do not need to import users from AD first for JIT provisioning to create Okta accounts.

If you do not have delegated authentication enabled, you must import the AD accounts first, and they must appear on the imported users list for JIT provisioning to create Okta accounts.

34) OUD Installation.

OUD 12C, JAVA DOWNLOAD, INSTALLATION AND CONFIGURATION
OUD Downloadable URL : Need to share URL with the team
Install JDK 1.8 (OUD 12c is only compatible with JDK 1.8)
Set the PATH and JAVA_HOME environment variables under system variables
path = c:\program files\java\jdk.18\bin
JAVA_HOME = c:\program files\java\jdk.18
Check the java installed or not by using "java -version" command in the command prompt
o/p : "java version "1.8.0_211"

OUD INSTALLATION:
unzip the OUD software
open powershelwindow (shift + right click and select open powershel window)
run the executable jar file as below
java -jar .\fmw_12.2.1.3.0_oud.jar (enter)
Follow the screenshots

OUD CONFIGURATION:
navigate to the oracle home
oracle_home : C:\Oracle\Middleware\Oracle_Home\oud
open powershel window (shift + right click on oud-setup batch file and select open powershel window)
run the batch file as below
.\oud-setup.bat (enter)
provide the required details (follow the screenshots)
HostName : localhost
Administration Port(s) : Enable Administration only with LDAP
LDAP Port : 4444
Admin port : is used to start or stop the OUD

services
LDAP port : is used for connectivity (eg: to connect with Okta etc)
Root User DN : cn=Directory Manager
Password : Welcome1
Password (confirm) : Welcome1
LDAP : Enable port on : 1389
Directory base DN : dc=kasi,dc=com
Creating instance directory C:\Oracle\Middleware\Oracle_Home\asinst_1\OUD ... Done

35) LDAP(OUD) Integration with Okta (LDAP Agent Installation and Configuration) in WINDOWS machine.

uid= xyz.abc, employeeType = contractor

Search base : ou=india,dc=vodafone,dc=cpm

F |
T = T

(T & F = F) (T & T = T)
(|(&(objectclass=*)(employeetype=emp))(&(objectclass=*)(employeetype=contractor)))

AND (&)

T & T = T
T & F = F
F & T = F
F & F = F

OR (|)

T | T = T
T | F = T
F | T = T
F | F = F

LDAP JIT and Delegated authentication
User creation in OUD
Default ports (LDAP : 389, SSL : 443, and Non-SSL : 80, Radius : 1812)

36) LDAP(OUD) Integration with Okta (LDAP Agent Installation and Configuration) in LINUX machine.

- Install OUD in Unix Server
- Install LDAP Agent in Unix server
- Configure LDAP in Okta then import users into Okta.
- will share the document for the same soon..

LDAP Agent Installation commands:
For RPM based machines:
yum localinstall OktaLDAPAgent_xx.xx.xx.x86_64.rpm

For Debian based Machines:
dpkg -i OktaLDAPAgent_xx.xx.xx_amd64.deb

1. To Check the OktaLDAPAgent Service status run:

   service OktaLDAPAgent status

2. To start the OktaLDAPAgent Service run:

   service OktaLDAPAgent start

3. To stop the OktaLDAPAgent Service run:

   service OktaLDAPAgent stop

Uninstall Okta LDAP agent
    yum remove OktaLDAPAgent

To check the logs : Navigate to agent installed location (cd /opt/Okta/OktaLDAPAgent/logs) then run below command
    tail -100f agent.log

RDP - To connect Windows Servers
Putty - To connect Linux/Unix servers

37) Attribute Level Mastering/Sourcing (ALM).

Attribute-level sourcing lets you specify different profile sources for individual user attributes. Without it, all of a user's attributes are provided by a single profile source.

38) Profile Masters/Source.

A profile source is an application that acts as a source of truth for user profile attributes. A user can only be sourced by a single application or directory at a time.

The priority determines which application or directory is considered the profile source for a user who is assigned to multiple profile source applications or directories.

39) Okta Expression Language.

- Expressions within mappings let you modify attributes before they are stored in Okta or sent to apps.

- Expressions allow you to reference, transform, and combine attributes before you store them on a user profile or before passing them to an application for authentication or provisioning.

For example, you might use a custom expression to create a username by stripping @company.com from an email address. Or, you might combine firstName and lastName attributes into a single displayName attribute

- Expressions allow you to concatenate attributes, manipulate strings, convert data types, and more. Okta supports a subset of the Spring Expression Language (SpEL) functions. For a comprehensive list of the supported functions, see Okta Expression Language. All functions work in UD mappings.

Reference URL : https://developer.okta.com/docs/reference/okta-expression-language/

40) Custom Attribute Creation and their Mappings.

We have 31 default base attributes for all users in an org.

Custom Attributes: Define additional attributes that are not available in the base attributes.

If we want to create any custom attributes in Okta profile, navigate to Directory >> Profile Editor >> Select Okta Profile >> Then click on Add Attribute >> then create attribute as per your requirement.

41) Group Rules.

Group rules simplify group administration and help you manage application access, application roles, and security policies. Below are the few advantages of using group rules.

- Automatically assign users to applications.
- Manage application assignments.
- Simplify the management of groups.
- Automate provisioning.
- Assign users to multiple groups.

Groups are commonly used for Okta single sign-on (SSO) access and to provision users to apps with specific entitlements. When you use rules to populate groups based on attributes, you achieve attributed-based access control.

The following are the group rules restrictions:

- Orgs (Okta Tenant) can have a maximum of 2000 rules.
- Group rules cannot be used to assign users to admin groups.
- You can only use string attributes in basic condition group rules.
- A group that is already the target of a group rule cannot be granted admin privileges.
- Only super admins and org admins can edit rules.
- Only group admins who manage all groups can search for and view rules. Individual group admins cannot search for or view rules.

42) Differences between Authentication, Authorization and Multifactor Authentication.

Authentication : The Process of providing the identity info (Username/Password) of a person or system. or Who are you? (Provide credentials)

Authorization : What can you Do? (What kind of privileges does user has).

Entitlements : Entitlements refer to the access rights, including group memberships or access permissions, that have been granted to a user who has an account on the related source. Eg : View, Create , Administrator etc..

Federation : The process by which an application/site requests proof of an authentication from a trusted source.

Federated Single Sign-On : The combination of a single

authentication event with multiple requests for proof of authentication.

43) Okta MFA (Multifactor Authentication).

Multifactor Authentication (MFA) is an added layer of security used to verify an end user's identity when they sign into an application or Okta.

MFA refers to a second layer of authentication (2FA), so usually an addition of information supplied beside the credentials (username, password);
but the difference between 2FA and MFA tends to be in the form of having a set of different factors from which you can choose one or even more that may coexist when speaking of MFA, and only one (usually; there can be more but they won’t coexist activated for the same user) when referring to 2FA;

44) Understanding different types of Applications

- Web Applications
- Mobile Applications
- Desktop Applications

45) Differences between Trusted and Target Apps.

The Trusted/authoritative application is the main repository for employee information for your enterprise, for example a human resources applications i.e. Workday, SuccessFactors, Ultipro, FieldGlass, PeopleSoft etc.)

Target/non-authoritative apps :- opposite to Trusted/authoritative apps. eg:- ServiceNow, Box, SalesForce etc..

46) Overview of Federation Concepts.

- IdP :Identity Provider (Okta)
- Sp : Service Provider (Application)
- Federation/SSO Protocols
  - SAML (Security Assertion Markup Language)
  - SWA (Secure Web Authentication) --- Specific to Okta
  - OIDC/OAuth (OpenID Connect)
  - Ws-Fed/Ws-Federation (Web Services Federation)

47) Understanding SAML Terms.
- doc shared

• Identity Provider Certificate : A self-signed X.509 certificate issued by IdP to sign or encrypt messages.
• Issuer : The unique ID of IdP that issues SAML assertion.
• Entity ID : The unique URL that identifies SP.

48) Understanding Okta applications and learn how to assign users to app in various ways.

- Assign individual users to the app in Assignments tab
- Assign Group to the app in Assignment tab
- Assign users by using API calls (Postman or Coding)

49) Outbound SAML Application integration with Okta (Using OIN).

The Okta Integration Network (OIN) is a catalog of thousands of pre-integrated applications to manage authentication and provisioning for all of your users.

Okta enables admins to provide SSO access to cloud, on-premise, and mobile applications. After the applications are configured, end users can sign into Okta and then launch any of their web apps without having to reenter their credentials.

- Requirement Gathering
  - Application Type (Web, Native/Mobile, SPA, OAuth Service based app)
  - SSO Protocols (SAML 2.0, OIDC/OAuth, WS-Fed)
    - granttype info (If it is OpenID/OAuth)
  - Do you have any lower environments to test
  - Metadata (App Urls)
  - User Provisioning (SAML JIT, API Provisioning)
  - Group info (User Access)
  - NameId - unique attribute and additional attributes, Group info
  - MFA requirement
  - Session Time Out
  - App login flows (IdP or Sp or Both)
  - Assertion Encryption (Certificate)
  - App Access (Internet vs Intranet)
  - Target completion date

- Test App SSO functionality in lower environments
  - Need to configure app in Okta lower environment with the above details.
  - Share the metadata with app team
  - Ask app team to configure app at their end
  - Ask app team to test the app functionality
  - Ask app team to provide UAT Sign-off

- Plan for production roll out
  - CR (Change Record), integration date and time:, UAT Sign-off, App owner approval, Okta Service owner approval
  - CAB calls - Seek approvals from CAB approvers
  - Setup a meeting with App team and exchange required details each other
  - Create app in Okta prod with required configurations
  - Send app integration confirmation email to management and app team
  - Ask app team to test the app functionality and seek confirmation mail.
  - Close the CR once app is integrated and confirmed by app team.

Signup for SalesForce admin trail version by using below link
https://www.salesforce.com/in/form/trial/freetrial/

App Name : SalesForce
Sp Initiated URL : https://voxxx.my.salesforce.com
IdP Initiated URL : https://dev-3xxx.okta.com

Username : manoj.mpxxxx@force.com
Password : Oxxx@123

App Name : DROP BOX :
URL: https://www.dropbox.com/login
asxxx@gmail.com
Okxx@123

SP URL : https://www.dropbox.com/sso/682090801951

App Name : ServiceNow
URL : https://www.servicenow.com/contact-us/sales.html#!

Single Logout (SLO): SLO is a feature in federated authentication where end users can sign out of both their Okta session and a configured application with a single action.

Okta supports this sign out process only when initiated by a Service Provider (SP). The SP sends the SLO request to Okta to end the Okta session.

- SWA applications don't support the SLO operation.
- SLO doesn't sign the end user out of other integrations that may be open.
- Okta doesn't sign out web applications.
- Not all app integrations support SLO. If the SP supports SLO in their downstream application, it is noted as a supported feature in their app configuration guide. Contact your SP directly to request that they add support for SLO.

For SAML applications, the SP must be able to send an SLO request to Okta as a POST request and it must be signed.

If you are using Okta for Single Sign-On (SSO) and you want to close and sign out of the Okta session, you can use the SAML Application Integration Wizard to configure SLO.

Logout Vs Single Logout

https://dev-3xxx.okta.com/login/signout

50) Outbound SAML Application integration with Okta (Using AIW).

If you want to add an integration/application that doesn't already exist in the Okta Integration Network (OIN), use the App Integration Wizard (AIW) to create a new app integration and connect Okta with your SAML, OIDC, SWA, or SCIM application.

51) Difference between JIT and SAML-JIT.

SAML JIT :- Use Just-in-Time (JIT) provisioning to automatically create a user account in your Application first time a user logs in with single sign-on (SSO).

JIT provisioning can reduce your workload and save time. JIT

provisioning also automatically applies password policies for your corporate network to your application, potentially increasing security.

With JIT provisioning, you can use a SAML assertion to create users the first time they log in to your application from a third-party identity provider. JIT provisioning saves you time and effort because it eliminates the need to provision users or create user accounts in advance.

For example, your company adds several new employees, and you want to create user accounts for them in your Application as soon as possible. You configure SSO and set up JIT provisioning. Now, when the new employees log in with SSO, the JIT provisioning method automatically creates their accounts.

JIT provisioning works with your identity provider to pass user information to Application in a SAML 2.0 assertion. You can create and modify accounts this way. Configure SAML settings for SSO in your Application before you set up JIT provisioning.

Note : JIT Provisioning cannot handle User deletion/deactivation in Application.

52) Usage of SAML Tracer, Fiddler Tracer and Developer Tools.

Download Fiddler tracer from google to see network traffic and SAML authentication request and Response etc.
Add SAML tracer extension to your chrome or FireFox browser to see SAML authentication request and Response
press F12 to open developer tools in your browser.

53) Understanding of Assertion, Metadata and Digital Signature.
- will share the doc

54) Different types of app login flows (IdP vs Sp Initiated).

An IdP-initiated login starts with the user first navigating to the IdP (like Okta) (typically a login page or dashboard), and then going to the SP with a SAML assertion.
In SP-initiated flow, user first hits application URL, then application redirect to IdP (SAML Authentication Request).
What's unique about the SP-initiated login is a SAML request.
There is no SAML Request/AuthN request involved in IdP-initiated flow, only SAML response is sent to SP.

55) SWA App integration.

Secure Web Authentication (SWA) is a form of authentication that provides single sign-on for apps that don't support proprietary federated sign-on methods or SAML/OpenID/Ws-Fed.
These credentials are stored such that users can access their apps without entering their credentials each time.
Okta Browser Plugin must be installed in our browsers for this protocol.

56) Overview of OIDC/OAuth protocols and sample app integration with Okta.

For theory, follow the shared doc

NODEJS WEB APPLICATION

Login URI : http://localhost:3000/callback
Logout URI : http://localhost:3000

node -v
git clone https://github.com/oktadeveloper/okta-nodejs-login-example.git
cd okta-nodejs-login-example
npm install

.env file in your root directory (C:\Users\Kaasi\okta-nodejs-login-example)
npm start

App signin URL: http://localhost:3000

Enable SLO for OIDC integrations

For OpenID Connect (OIDC) integrations, the SP application must be configured to send an SLO request to Okta as a GET request. The application should redirect to this Okta endpoint:

GET https://{baseUrl}/logout?id_token_hint=${id_token}&post_logout_redirect_uri=${post_logout_redirect_uri}&state=${state}

Where:
baseURL is the URL for your Okta org.
id_token is the OIDC token issued by Okta during sign on.
Optional. The post_logout_redirect_uri is the Logout redirect URI where Okta redirects the user after the SLO operation. This URI must be listed in the Logout redirect URIs configuration in the General Settings for your Okta integration.
Optional. The state is any string to be added as parameter upon redirect to the SLO URI.
After this request is processed, the id_token is invalidated and the user is signed out from Okta.

For more details on the GET request to the API, see the OpenID Connect & OAuth 2.0 API reference.

For application developers, language-specific instructions are also available in our Sign users out developer guide.

Finally, you need to add the Logout redirect URIs to your Okta integration:
In the Admin Console, go to Applications > Applications.
Click the OIDC application where you want to add SLO.
In the General settings tab, click Edit.
Beside the Logout redirect URIs, click + Add URI.
Enter the URI where Okta will send relying party-initiated SLO requests.
Click Save.
To test your SLO flow, sign in to your SP application using the Okta integration and then use the appropriate sign out method from within the SP application. The browser should sign you out of both your SP application and

57) Overview of Ws-Fed protocol and sample app integration with Okta
- Follow the doc

58) Overview of SCIM (System for Cross Domain Identity Management) and OPP agent installation.
- Follow the doc

59) Install and configure the Okta RADIUS Server agent and RADIUS App Configuration.
- Follow the doc

60) Okta Logs (User, application, AD, LDAP, Radius server logs).

System Log

The System Log contains details of all logged events for your org. View and monitor various events in your org using:

- Graphs
- Events Table
- Filters and search

To navigate to the System Log, in the Admin Console, go to Reports > System Log.

Graphs

The System Log displays the bar graphs about your chosen events:

- Count of events over time
- Count of events by category

Click the Count of events by category link to expand the graphs:

- Count of events for each target
- Count of events for each actor
- Count of events for each event type

For more information about a data point, hover over any of the bars in the graphs. Narrow the time range of a graph by dragging your mouse over the bars to grab the range you are interested in.

Events Table

Event Table lists all events and includes information about time, actor, target, and more.

You can:

- View more data about an event by clicking the right arrow on the corresponding row.
- Filter events by Time, Event Info, Actor, or Targets in the table by clicking on the column header.
- Download the entire table by clicking the Download CSV file link.
- Toggle between the table view and a geolocation view, which displays events on a map.
- Access the Rate Limit Dashboard using the using the link provided in the rate limit violation event. See Rate Limits Dashboard.

Filters and search

You can filter events by various parameters and operators in the System Log. By default, the filters display all events for the last seven

days. See System Log filters and search for more information.

61) Understanding of Chiclets/App tile and Okta Mobile Management (OMM).

Chiclet :- A obsolete term for the application icons that appear on an end user's Home page. The terms has been replaced by "apps” or “icons.”

Okta Mobility Management (OMM):- OMM allows you to manage your end users' computers, mobile devices, applications, and data. Your end users enroll in the service and can then download and use managed apps from the Apps Store. Managed apps are typically work-related, such as Box or Concur. As an administrator, you can remove managed apps and associated data from end users' devices at any time. You can configure policies, such as data sharing controls, on any of your managed apps.

62) Okta Self Service.

SSPR - Self Service Password Reset

Self-service registration (SSR) lets users use a custom app or the Okta Homepage to self-register. After you enable SSR, a Sign up link appears in the Okta Sign-In widget. Users who select this link are directed to a new Create Account registration form based on a customized registration policy.

63) Understanding of Application self service functionality and how to make application as self service.

Software that allows users to request access to resources using a self-service interface, which uses workflow to route the request to the appropriate manager(s) for approval.

64) Okta Desktop SSO/ IWA (Agent based vs Agent less)

https://help.okta.com/en/prod/Content/Topics/Directory/ad-iwa-learn.htm#:~:text=The%20Okta%20IWA%20Web%20agent%20is%20a%20lightweight%20Internet%20Information,sign%20into%20your%20Windows%20network.

- Agent based IWA

DSSO allows users to be automatically authenticated by Okta and any apps accessed through Okta, whenever they sign into your Windows network.

The Okta IWA Web agent is a lightweight Internet Information Services (IIS) web agent that enables Desktop Single Sign-on (DSSO) on the Okta service.

The Okta IWA Web agent uses Microsoft's IWA and ASP.NET to authenticate users from specified gateway IPs.

- Agentless IWA

With agentless Desktop Single Sign-on (DSSO), you don't need to deploy IWA agents in your Active Directory domains to implement DSSO functionality. This reduces or eliminates the maintenance overhead and provides high availability as Okta assumes responsibility for Kerberos validation.

65) Understanding High availability and Load balancing.

High availability :-

In computing, the term availability is used to describe the period of time when a service is available, as well as the time required by a system to respond to a request made by a user. High availability is a quality of a system or component that assures a high level of operational performance for a

given period of time.

Load balancing :-

Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers

A load balancer performs the following functions:

Distributes client requests or network load efficiently across multiple servers

Ensures high availability and reliability by sending requests only to servers that are online

Provides the flexibility to add or subtract servers as demand dictates

Load Balancing Algorithms

Round Robin – Requests are distributed across the group of servers sequentially.

Least Connections – A new request is sent to the server with the fewest current connections to clients. The relative computing capacity of each server is factored into determining which one has the least connections.

Least Time – Sends requests to the server selected by a formula that combines the fastest response time and fewest active connections.

Hash – Distributes requests based on a key you define, such as the client IP address or the request URL.

IP Hash – The IP address of the client is used to determine which server receives the request.

Random with Two Choices – Picks two servers at random and sends the request to the one that is selected by then applying the Least Connections algorithm

Benefits of Load Balancing

Reduced downtime
Scalable
Redundancy
Flexibility
Efficiency

Failover :-

Failover is a backup operational mode that automatically switches to a standby server or network if the primary system fails, or is shut down for servicing.

Failover is an extremely important function for critical systems that require always-on accessibility.

Failover functionality seamlessly redirects requests from the failed or downed system to the backup system that mimics the operating system environment.

66) Configuring IDP and Routing rules in Okta.

Identity Provider (IdP) routing rules enable you to direct end users to identity providers based on the user's location, device, email domain, attributes, or the app they are attempting to access. This feature is also known as IdP Discovery, because these routing rules allow Okta to discover which identity provider to use based on this context.

67) Inbound SAML app integration (Org2Org Setup).

- Create Org2Org app in IDP Okta (Follow "view setup instruction" guide for required URLs/Values)
- Enable Provisioning if required.
- if provisioning is needed, create an API token (With Super Admin privileges) in SP Okta and configure it in IDP Okta.
- Add an Identity Provider and configure in SP Okta (Follow "view setup instruction" guide for required URLs/Values).
- Create and configure routing rule in SP Okta for IDP Okta (based on attribute or anything)
- Assign required users/groups to the Org2Org application in IDP Okta. these users get created in SP Okta.
- Push groups from IDP Okta to SP Okta if required.
- Assign these users/group to any applications that are available in SP Okta to provide access to IDP Okta Users.
- Now these users will be redirected to IDP Okta for an authentication whenever they are trying to acceess any applications which are integrated in SP Okta.
- Create a bookmark application in IDP Okta to accees SP Okta protected applications directly from IDP Okta end user Dashboard.

IDP Sign on Url + ?RelayState= + Embedded link of the application in the SP Okta

https://dev-982844.oktapreview.com/app/okta_org2org/exk10jz6fvmPWS89f0h8/sso/saml?RelayState=https://dev-63389365.okta.com/home/salesforce/0oa15wope1uONCDx35d7/46

Eg:

http://sourceorg.okta.com/app/okta_org2org/exkidkmZXAoxbgwz20g3/sso/saml?RelayState=http://huborg.okta.com/home/google/0oaiqwYT8RpdS8I6D0g3/26

68) Application Provisioning and mappings.

Enable Provisioning in app provisioning tab and do the appropriate mappings in Profile Editor as per business requirement.

69) What is Group Push?

Group Push lets you push existing Okta groups and their memberships to provisioning-enabled, third-party applications. These memberships are then sourced by Okta.

Pushed groups are managed from Okta. Making changes to the group in the target app causes synchronization issues with Okta.

Groups are pushed to applications using one of the following two methods:

By name: An Okta application administrator selects groups from Okta to be created and updated in the target app.
By rule: You use a string in either the group name or description

to push many groups at once. Group push by rule is not available for AD integrations.

The following are the known Group Push limitations:

Using the same Okta group for assignments and for group push is not supported. To maintain consistent group membership between Okta and the downstream app, you need to create a separate group that is configured to push groups to the target app.

70) Create and understand Okta policies (Authentication, Password, MFA and App Sign-On Policies) and understanding of Okta Session timeouts.

About Policies :

- Policies help you manage access to your applications and APIs.
- Policies are evaluated when an access request is made.
- A policy contains a set of rules which define permissions that determine whether the request is allowed or denied.
- Policies are group-scoped and rules are context-scoped.
- Different policy types share a common framework but have different policy settings and rule data.

Policy Types :

Okta Sign-On Policy : Determines who can sign in and how a user is allowed to sign into Okta, including control of MFA enforcement.

Under Security >> Authentication > Sign On

Okta sign-on policies can specify actions to take, such as allowing access, prompting for a challenge, and setting the time before prompting for another challenge. You can specify the order in which policies are executed and add any number of policies. If a policy in the list does not apply to the user trying to sign in, the system moves to the next policy.

Password Policy : Governs password complexity and age, account lockout, and self-service recovery options.

Under Security >> Authentication > Password

Password policies enables admins to define password policies and associated rules that enforce password settings at the group and authentication-provider level. Okta provides a default policy to enforce the use of strong passwords to better protect your organization's assets. Admins can also create additional policies that are less or more restrictive and apply them to users based on group membership.

Multifactor Policy : Controls when, where and which factors may be used for enrollment.

Under Security >> Multifactor >> Factor Enrollment

Use the Multifactor Policies tab to create and enforce policies for your chosen MFA factors and the groups that are subject to them. Sign-on policies determine the types of authentication challenges these users receive.

Application Sign-On Policy : Determines the extra levels of authentication that you can add before an application can be accessed, also includes control of MFA enforcement.

Under Applications >> Specific app Sign On policy
App sign-on policies allow or restrict access to applications. By default, all Client options in the App Sign On Rule dialog box are pre-selected. To configure more granular access to the app, selectively apply conditions as you create one or more prioritized rules

How Are Policies Evaluated? :

- Policies are evaluated top down
  - The first policy to have its criteria met is the one applied
  - Subsequent policies are ignored
- Primarily based on group membership
  - A policy can be associated with one or multiple groups.
- In general, the most restrictive policy should be ordered to evaluate first.

Policy Rules :

- Like policies, rules are evaluated top down
- Based on context, primarily client IP address
  - Can be in or not in a zone
- In general, the rules with the narrowest criteria should be ordered to evaluate first.
- A policy with no rules cannot be applied.

71) Okta Network Zones.

A Network Zone is a security perimeter to limit or restrict access to a network based on a single IP address, one or more IP address ranges, or a list of Geo-locations.
Network Zones are defined and maintained by admins who wish to improve and strengthen network security for their organization and users.

Network Zones consist of IP Zones and Dynamic Zones:
An IP Zone enables admins to define network perimeters around a set of IPs. Admins can add both Gateway IPs and Proxy IPs to IP Zones.
Dynamic Zones enable admins to define network perimeters around location, IP Type and Autonomous System Number (ASN).

Both IP Zones and Dynamic Zones have the following limitations:

Up to 100 zones configured per org
Up to 150 Gateway IPs and 150 Proxy IPs (except for IP zones that are blocked)
IP blocked zones may contain up to 1000 gateways per zone and up to a total of 25,000 per org

To Know your public ip :- type "what's my ip" in Google

To calculate CIDR notation IP's :- https://www.ipaddressguide.com/cidr

72) Use and advantage of Okta Device Trust.

Okta Device Trust contextual access management solutions enable

organizations to protect their sensitive corporate resources by allowing only end users and partners with managed devices to access Okta-integrated applications.

https://help.okta.com/en/prev/Content/Topics/Mobile/Okta_Mobile_Device_Trust_Windows-desktop.htm

73) Okta Automations.

Automations allow you to create automated actions that run based on a set of trigger conditions.
Okta Automations enable you to prepare and respond to situations that occur during the lifecycle of end users who are assigned to an Okta group.

Okta Automations for active users :-
Okta Automations looks for active users who have not logged into Okta for a set number of days. For Automations, an active user refers to a user with an active Okta account. Accounts become active when:
Admins add a user (Add Person) in the Manage users page and you set the user password without requiring email verification.
An end user self-registers into your custom app or the Okta Homepage and email verification is not required.
Admins explicitly activate user accounts.

Okta Automations for inactive users
Users are considered inactive if no activity is detected on an active account for a defined number of days. For example, if a user is inactive for a defined number of days and is on the verge of being locked out, an automation can send an alert to the inactive user in advance

74) Overview of Inline and Event Hooks.
- Follow the doc

Inline hooks allow you to connect your org to external services to make requests that can modify Okta's behavior
Event hooks send event data from Okta to an external endpoint when a selected event occurs

75) Understanding Okta Reports and how to generate custom reports.

Use the Reports page and System Log to monitor activity and security of your org. The Reports page contains canned reports and pre-defined System Log queries to help admins detect potential security risks and understand how apps and services are consumed by end users.

Reports : https://help.okta.com/en/prev/Content/Topics/Reports/report-types.htm
System Log filters and search : https://help.okta.com/en/prev/Content/Topics/Reports/syslog-filters.htm
Default Okta Log retention period : 3 months

76) Okta Appearance and UI Customizations.

- App Theme colors (Under Settings >> Appearance)
- Branding (Logo) (Under Settings >> Appearance)
- Login page (Under Settings >> Customization)
- Optional User Account Fields (Under Settings >> Customization)
- Sign-Out Page Configuration (Under Settings >> Customization)

- Okta Interstitial Page (Under Settings >> Customization)
- Application Access Error Page (Under Settings >> Customization)
- New End-User Experience (Under Settings >> Customization)
- Reauthentication Settings (Under Settings >> Customization)
- Email and SMS template changes (Under Settings >> Email & SMS)
- Custom email domian settings (Under Settings >> Email & SMS)
- Organization Contact (Under Settings >> Account)
- End User Support (Under Settings >> Account)
- Rate Limit configurations (Under Settings >> Account)

Rate limiting is used to control the amount of incoming and outgoing traffic to or from a network. For example, let's say you are using a particular service's API that is configured to allow 100 requests/minute. If the number of requests you make exceeds that limit, then an error will be triggered. The reasoning behind implementing rate limits is to allow for a better flow of data and to increase security by mitigating attacks such as DDoS.

https://developer.okta.com/docs/reference/rate-limits/

77) How to check Okta Version and how to raise a support case with Okta vendor.

mail to : support@okta.com
To open a case with Okta Vendor : https://support.okta.com/help/s/opencase
Give Access to Okta Support under Settings >> Account submenu

78) Enabling EA features.

Enable it under Settings >> Features submenu

Features in Early Access ('EA') are new or enhanced functionality available in both Production and Preview orgs.

It is best practice to enable and test features in your Preview org before enabling in Production.

79) Okta Notifications and Agent Health checks.

Configure Admin Email Notifications under Settings >> Account submenu
Check Agents health under Directory >> Directory Integrations >> AD/LDAP >> Agents

80) Understanding Okta Healthinsight and ThreatInsight.

Healthinsight: (Under Security >> HealthInsight)

HealthInsight audits an organization’s security settings and suggests recommended tasks to improve security posture. These security recommendations are intended primarily for admins that manage employees within their organization.

https://help.okta.com/en/prod/Content/Topics/Security/healthinsight/healthinsight-security-task-recomendations.htm

ThreatInsight : (Under Security >> General)

The detection of a threat takes place prior to authentication evaluation. Requests that are blocked by Okta ThreatInsight prevent user lockouts from suspicious IP addresses. Configure Okta ThreatInsight to detect suspicious IP addresses from credential-based attacks.

When Okta ThreatInsight actions are enabled, end users may sign in to their org as usual. If a sign-in attempt from a malicious IP address is

detected and authentication requests are set to be blocked, the user receives an HTTP 403 error.

Okta ThreatInsight is just one tool in the security toolbox and blocks certain malicious traffic. It cannot guarantee 100% malicious IP address detection or 100% threat detection

https://help.okta.com/en/prod/Content/Topics/Security/threat-insight/about-threatinsight.htm

81) Uninstalling and Reinstalling the AD/LDP/IWA/RADIUS Agents.

Uninstallation: Eg for AD agent
Log into Okta >> Navigate Directory >> Directory Integrations >> Active Directory >> Agents >> Deactivate Agent
Log into Agent installed server >> Open control pannel >> Programs and features >> right click on Okta AD agent then click on uninstall
Open C drive >> Program files x86 >> remove Okta folder
make sure Okta AD agent service should not available in Services.
Now start the installation procedure

82) Configuring AD is normal application.

Install the AD agent
Makesure AD agent service account should have admin privileges to create users in AD.
Navigate to Directory >> Directory Integrations >> Active Directory >> Provisioning >> To App >> Enable Create users, update user attributes and Deactivate users then save it.
Create any group under Directory >> Groups (Eg : Test AD Provisioning Group)
Open Test AD Provisioning Group >> Directories >> Manage directories >> Select AD Domain >> Next >> Select OU and confirm changes
Now try to add user to Test AD Provisioning Group, user should create in AD under specified OU.
We can enable Group Push as well.

83) Advanced Server Access.

Okta Advanced Server Access is an application that manages SSH and RDP access to Linux and Windows servers. Using Okta as its source of truth, Advanced Server Access reconciles with your internal servers to provide Zero Trust software that you can use to secure them. To start using Advanced Server Access, you create a team and configure some settings. In Advanced Server Access, a team is a named group of users who can authenticate with Okta. A team is an Advanced Server Access tenant, which is similar to an Okta tenant. All configurations and resources in Advanced Server Access are scoped to a team.

https://help.okta.com/en/prod/Content/Topics/Adv_Server_Access/docs/asa-overview.htm

https://app.scaleft.com/

https://help.okta.com/en/prod/Content/Topics/Adv_Server_Access/docs/sft-windows.htm download link 1.1.45

https://help.okta.com/en/prod/Content/Topics/Adv_Server_Access/docs/client.htm

- Create app in Okta (Follow "view setup instructions")
- Enable Provisioning
- Download ScaleFT software (https://dist.scaleft.com/client-tools/windows/latest/ScaleFT.msi)
- enroll client (run this command in command prompt -> sft enroll)
- All enrolled clients will be appear under your profile in ASA clients console

84) Okta basic troubleshooting steps, my recommendations and best practices.

Okta basic troubleshooting steps :

- if user is unable to access an Application
  Use SAML tracer or Fiddler tracer to see the network traffic
  Check user logs in Okta and AD/LDAP/RADIUS agent logs
  Check if user has valid profile in Okta
  Check if user is assined to the application or not and user is having valid group membership or not.
  Check if user is having all required attributes in Okta profile to send details in SAML assertion.
  Check Okta tasks if user is having any provisioning/assignement related issues
  If everything looks fine at Okta end, check with application team if that user is availale in their app or not.

- Validate Okta expression language by creating dummy application in Okta
- Check App and Okta Sign on policis and their session time outs
- If user is unbale to import from LDAP/AD even though user has all required attributes.
  Check okta logs and AD/LDAP logs why user is skipping during the import
  check LDAP user search filter if that user is satisfying that filter rule or not by using any LDAP browsers
  Check user in LDAP/AD if user attributes having any weird characters

- Still if you are unbale to find any resolution for the issue, escalate it to your next team else raise an Okta support case.

My recommendations and best practices :

- Create atleast 2 super admin accounts in Okta. if something goes wrong with one super admin account we can use other account to access Okta.
- Install multiple agents (AD/LDAP/RADIUS/IWA/OPP) to maintain high availablity and better performance.
- Use different service accounts (Okta local accounts with super admin privileges with pwd set to never expire) to install any agents. it avoids dependancy on individual users.
- Always take a backup before we modify any configurations (Policies, email templates, agent config file etc)
- Never ever perform any write actions (any modifications) in Okta production without having proper approvals from your supervisor and service owner.
- Always test end to end (thoroughly) any functionality before move this feature/Configurations to Production.
- Complete your tasks/work within defined SLA(Service Level Agreement).
- Discuss with your team and supervisor before taking any action in Okta.
- Don't give super admin or any admin privileges to anyone until and

unless you have valid approvals.
- Never share any API tokens to anyone. if app team/anyone requests for it, seek approvals from Okta service owner and share API token with him (one to one)

85) Real time Project explanation.

86) Okta support/developer sites.

https://support.okta.com/help/s/
https://developer.okta.com/
https://help.okta.com/en/prod/Content/index.htm

87) Providing required Documents.
88) All Topics revision (Q/A).
89) Interview questions.
- Doc Shared
90) ================================== THE END ==================================