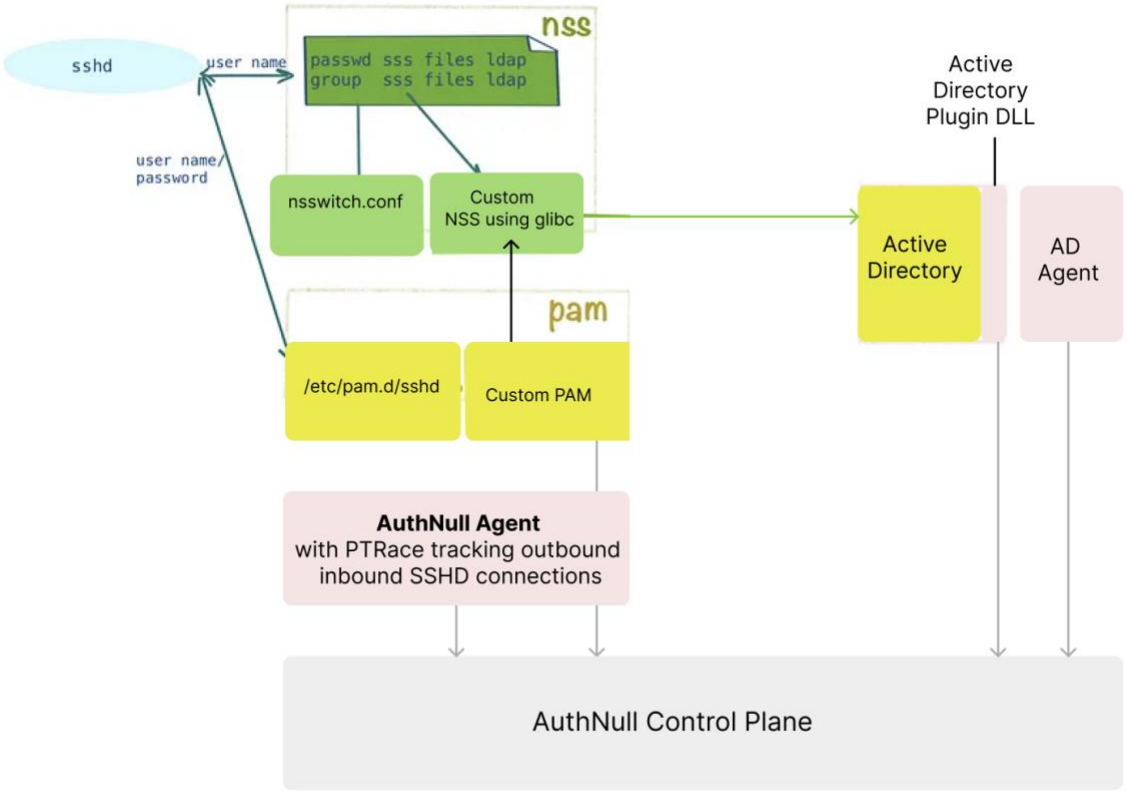
Logical and Physical Architecture

AuthNull

Table of Contents

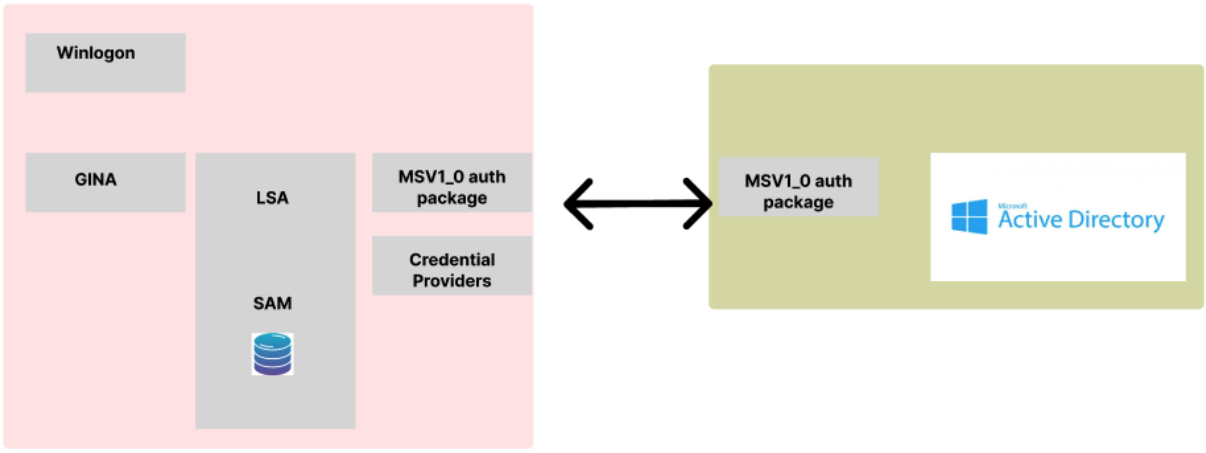
Linux control plane – Logical external components



Component	**Purpose**
Custom nss with glibc Nsswitch conf file Or SSSD config	Use nsswitch.conf to locate ldap server to verify identity of the user Used to authenticate against active directory.
Custom pam with SSHD config	Trigger Passwordless authentication
AuthNull Agent using Ptrace	Discover local accounts, service accounts, groups Ptrace is used to Track outbound / inbound connections for the purpose of

App. Env is a dependency which has an machine key to communicate with the server	identifying interactive or m2m authentication

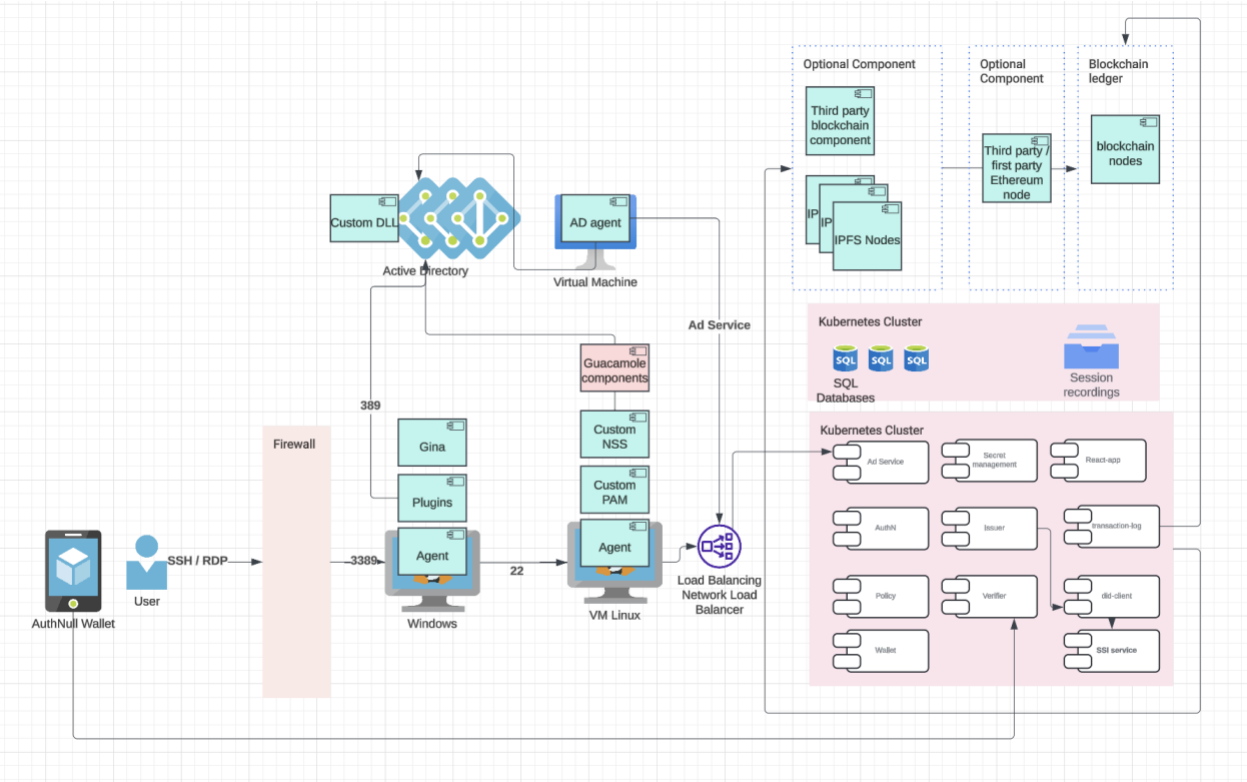
Windows control plane - Logical external components



Component	**Purpose**
Gina	GINA (https://learn.microsoft.com/en-us/windows/win32/secauthn/gina) modification is done together which does a take over of the logon screen.
Plugin – LDAP credential provider	Calls the LDAP server for LDAP authentication Calls the AuthNull / SSP server for Passwordless authentnication
AuthNull Agent using Ptrace App. Env is a dependency which has an machine key to communicate with the server	Discover local accounts, service accounts, groups Ptrace is used to Track outbound / inbound connections for the purpose of identifying interactive or m2m authentication
Plugin – Local credential provider	Calls the Local machine for local user authentication authentication

	Calls the AuthNull / SSP server for Passwordless authentnication
Plugin – Kerberos auth	Enables Kerberos authentication
Plugin – Radius Auth	Enables Radius authentication

AuthNull Physical architecture

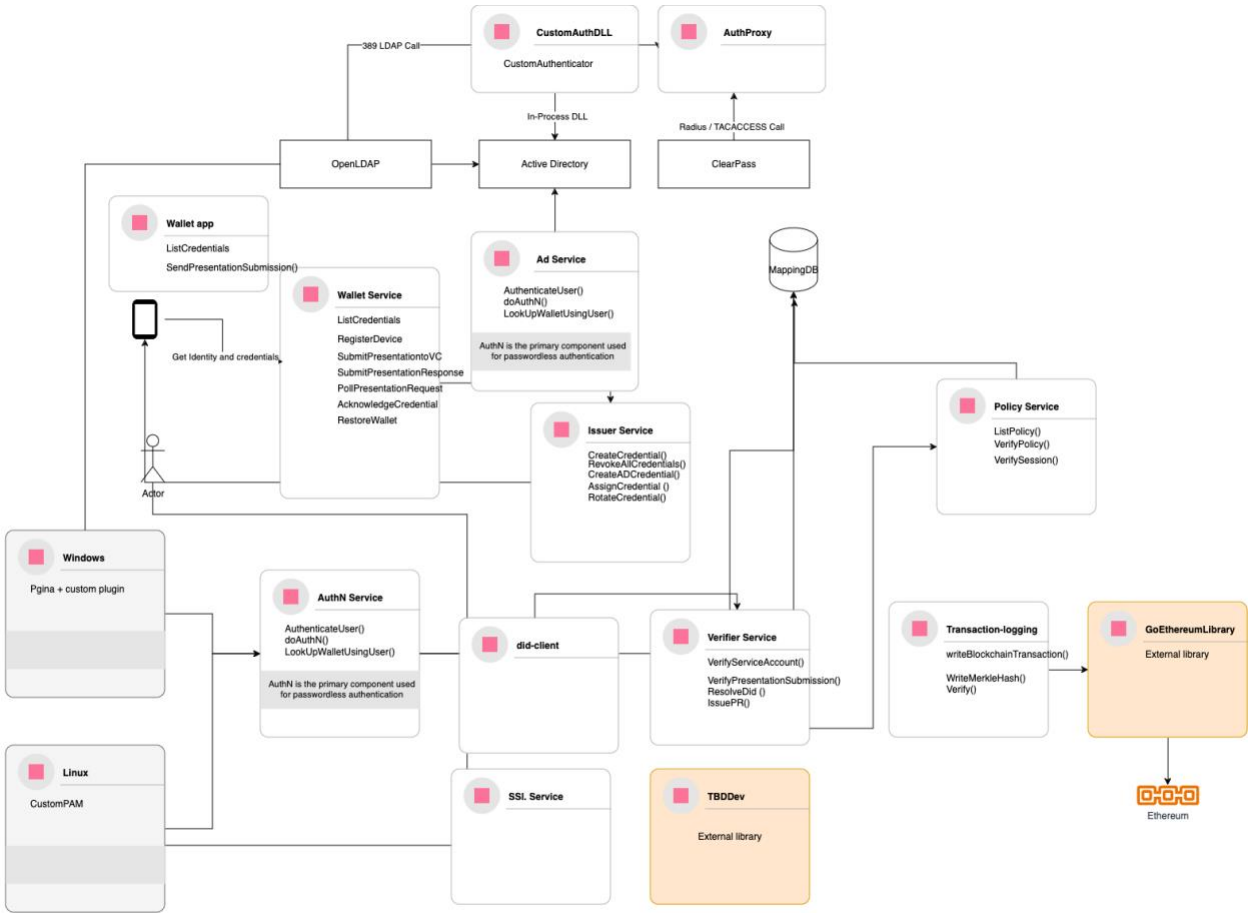


Component	**Purpose**
Client side components for Windows and Linux	As discussed in previous sections
Bastion host components	A bastion host (suggested 2) has components using the open source tools

	– Guacamole / modified to be used with AuthNull. Guacamole offers remote secure tunnel together with session recording capability.
Wallet	React Native Wallet for iOS and Android App
GKE microservices	Various microservices as listed in the inventory sheet correspond to various functions that AuthNull platform uses
Load balancer	A simple load balancer that can balance out load on GKE microservices
Postgres Cluster	Postgres cluster on GKE using Postgres Operator Uses a special extension for Graph dB search for Identity tapestry project.
Third party libraries (APIs) for Blockchain	Example Etherscan api provider among others can provide an API (write throttled) to be able to write to Ethereum or L2 network
Self managed or third party managed node	This can be introduced to improve write latencies to Ethereum – along with other advanages. - node verifies all the transactions and blocks against consensus rules by itself. .. - You can use an Ethereum wallet with your own node. ... - Provide your own custom RPC endpoints.
Blockchain itself	This can be Ethereum, or an Ethereum L2 node, or completely different blockchain like solana.

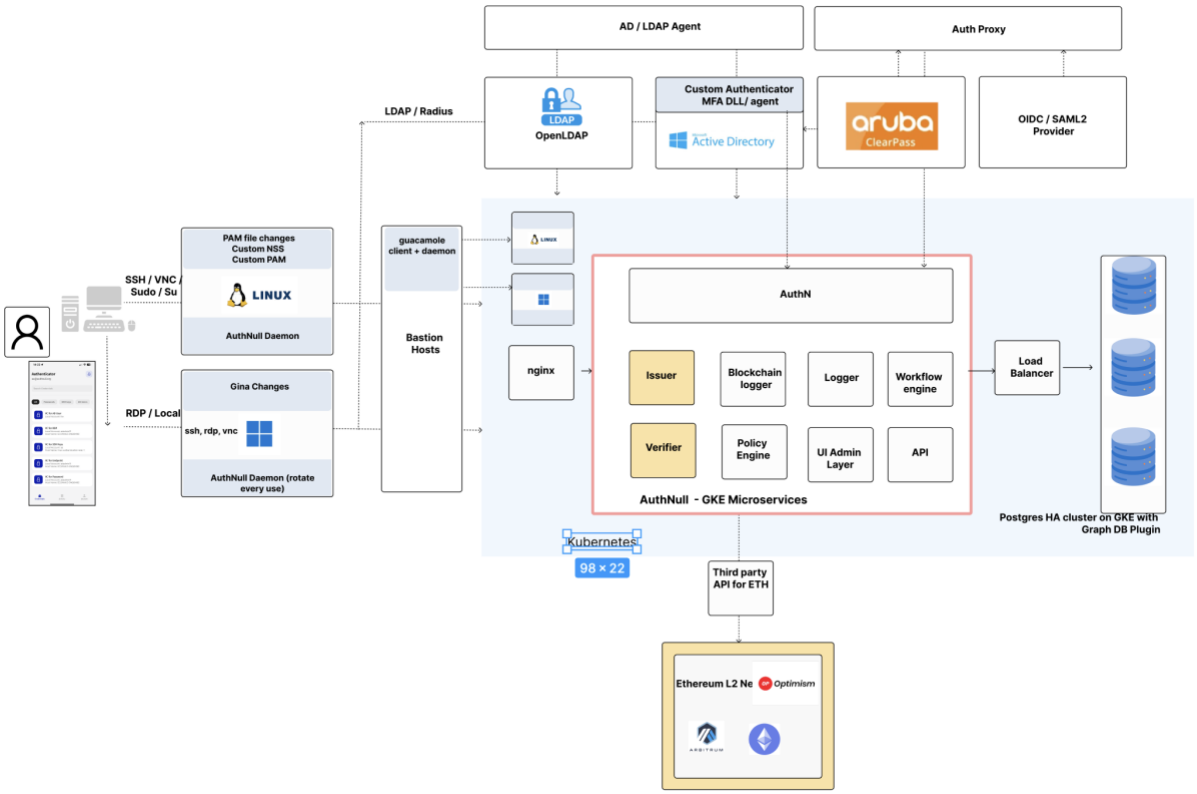
	See solution overview doc for comparisons between various blockchain options.
Ad agent	This is the agent(s) that runs on a virtual machine near the Active directory nodes. These agent sync active directory to the main control plane. The agent - Discovers users; service account users - Rotates credentials - Discovers default policies - Triggers user onboarding / offboarding when new users are onboarded and offboarded. -

Component Diagram



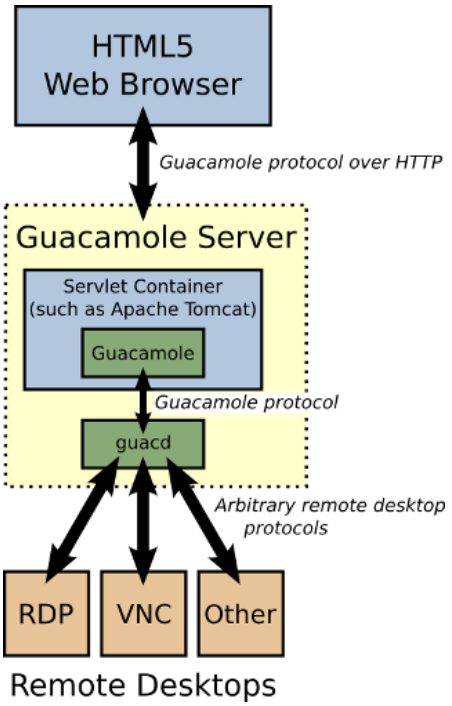
Component	Purpose
Policy service	List policies. Check for policies
Wallet service	Communicate with wallet. Send credentials. Respond to wallet request.
Issuer service	Issue credentials and VCs
Verifier service	Verify identities, credentials and identities
Policy service	List policies, verify sessions and verify policies
AuthN	Primary authentication service used by all client side components
Transaction logging service	Write to blockchain as single transaction hash, merkle hash tree
GoEthereum library	The current library that is used to write to the Ethereum blockchain.
AD Agent	Agent that runs near the active directory to synchronize active directory users
Custom Authenticator DLL	MS_V1. Authenthicator custom auth package DLL that runs in process within Active directory for agentless operations for MFA.
Auth Proxy	Used for MFA from Radius / Open LDAP (replacement for Active directory).
SSI Service	Forked from TBD Dev The Self Sovereign Identity Service (SSIS) facilitates all things relating to DIDs and Verifiable Credentials -- in a box! The service is a part of a larger Decentralized Web Platform architecture which you can learn more about in our collaboration repo. The SSI Service is a HTTP-API driven web service that wraps the ssi-sdk

Logical architecture



AuthNull is a microservices based architecture that is typically deployed on a Kubernetes microservices.

Component	Purpose
Wallet	Client side component wallet and authenticator app. on IOS / Android. Required on MacOS, Browser Extension.
Linux Components	Ptrace module for SSHD Agent Custom PAM Custom NSS Shell script
Bastion host components	Apache guacamole – guacd server Servlet / client
Windows Components	PGina Custom authenticator plugin for LDAP

	Powershell script Agent
Bastion hosts	Guacamole which consists of Guacd server Guacamole client 
Loadbalancer	Nginx or equivalent
GKE Microservices	AuthN service Blockchain logger Logger service Workflow engine UI admin layer Verifier Policy engine Issuer SSI Service Other microservices.
Blockchain external library	GoEthereum, or any other third party library.
Database	Postgres Cluster
Other components	OpenLDAP GlAuth Freeradius