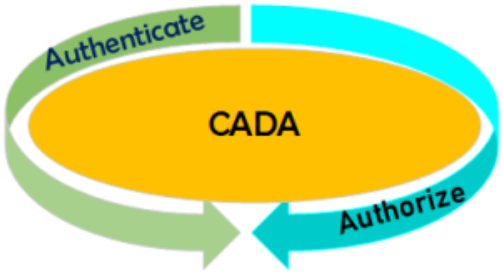
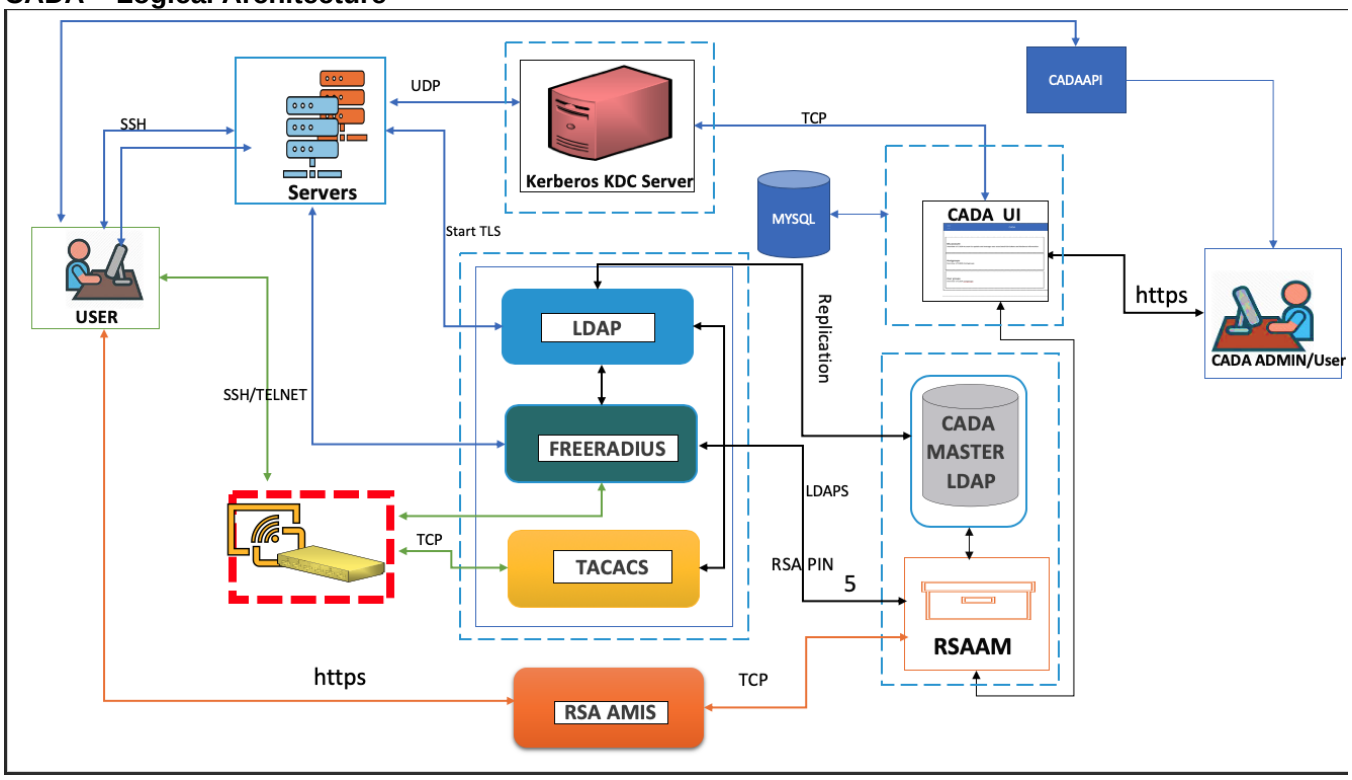
CADA Architecture and Diagrams



CADA Architecture and Diagrams

Table of Contents

CADA – Logical Architecture



Server Authentication Flow

1.1 User tries to login to a server using **SSH.**

1.2 The Server validates the User's password against the **Kerberos KDC Server**.

1.3 If the **Kerberos** authentication was successful, the Server authorizes the User's access to Server by checking against the **AAA LDAP**. User must be

part of server's host-access container. Server opens a session for the User if authorization is successful

1.4 Alternatively**,** if the server is enabled with **2FA (Two Factor Authentication)**, User must provide additional **RSA** passcod e credentials. The Server validates the **RSA** passcode against

RSA Authentication Manager(RSAAM).

1.5 The request to **RSAAM** is proxied through the **AAA Freeradius** Server.

Network Device Authentication Flow

2.1 User tries to access a network device

2.2 The device prompts the user for the **RSA** pass-code and sends it to **AAA Freeradius** for validation.

2.3 Freeradius validates the user credentials against **RSAAM.**

2.4 In case the device is configured for only radius authorization using **Vendor Specific Attributes (VSA), Freeradius** fetch es the **VSA** from **LDAP** and sends it back to the device. Upon successful authentication and authorization the device opens a session for the user.

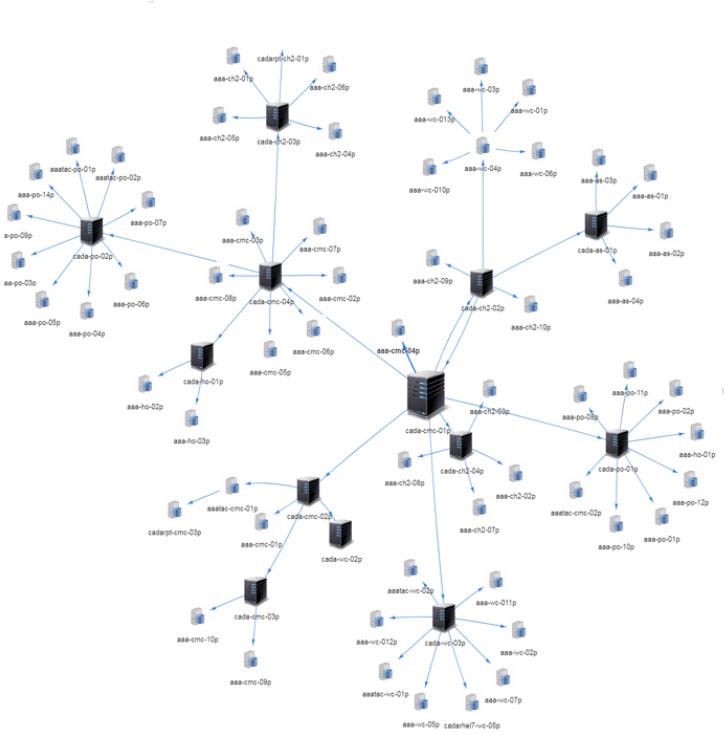
2.5 In case the device is configured for **TACACS** style command authorization, the device reaches out to the **AAA TACACS** server for authorizing every

command the user tries on the device.

2.6 AAA TACACS server checks the command authorization against the **LDAP** and allows the command to run if authorization is successful.

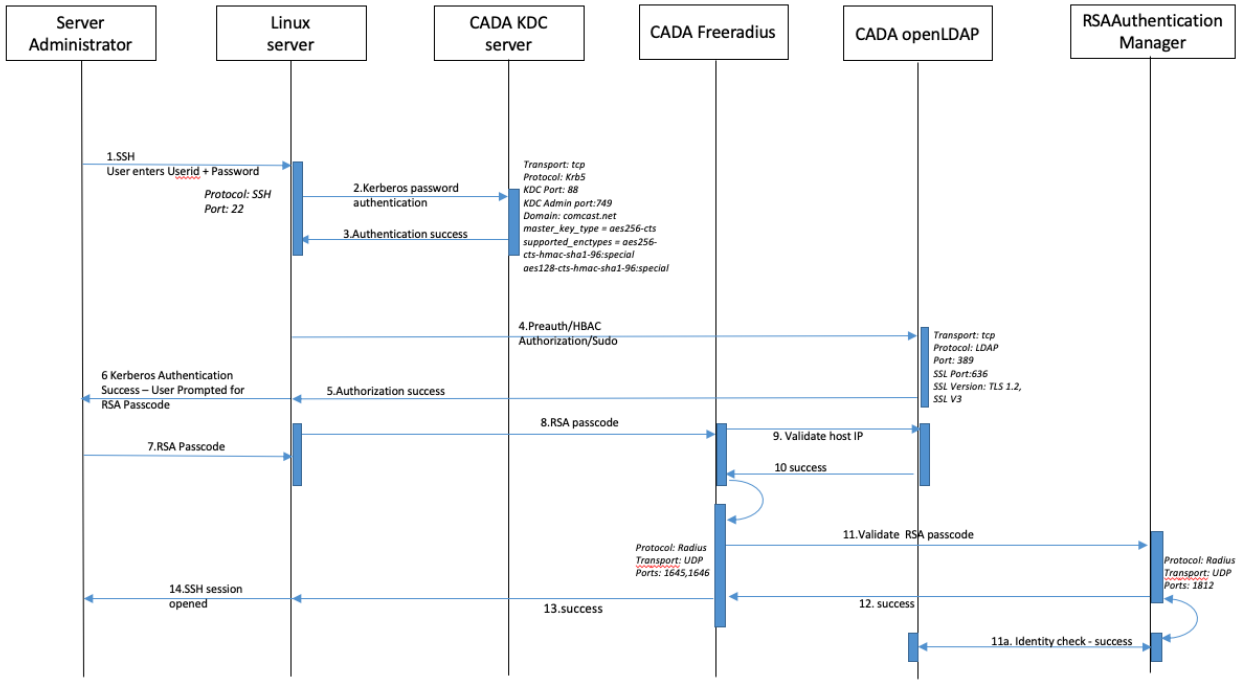
CADA – Physical Replication Layout

The below diagram captures the physical architecture of the CADA LDAP and the AAA servers across the different data centers. The LDAP changes on the master CADA are automatically replicated to the local CADA masters in datacenters and then to the respective AAA servers.



CADA - Network Device authentication/authorization

CADA - MFA Server Authentication Flow



GO BACK TO

E-CADA main page CADA Home Page