Kerberos

Serviciu de autentificare pentru sistemele distribuite

Într-un mediu personal, neconectat la rețea, resursele și informațiile pot fi protejate prin securizarea fizică a calculatorului personal. Într-un mediu de calcul partajat (sistemul de operare împarte o mica porțiune a calculatorului fiecărui utilizator), sistemul de operare protejează utilizatorii unul de celălalt și controlează resursele. Pentru a determina ce poate citi sau modifica fiecare utilizator, este necesar ca sistemul să identifice fiecare utilizator. Acest lucru se realizează atunci când utilizatorul se autentifică.

Într-o rețea de utilizatori care necesită servicii de la mai multe computere separate, există trei abordări pentru controlul accesului: se poate să nu se facă nimic, bazându-se pe mașina la care utilizatorul este conectat pentru a preveni accesul neautorizat; se poate cere host-ului să-și dovedească identitatea, dar să se bazeze pe acesta cu privire la identitatea utilizatorului; sau se poate cere utilizatorului să-și dovedească identitatea pentru fiecare serviciu necesar. Serverul trebuie, de asemenea, să-și dovedească și el identitatea.

Într-un mediu închis în care toate mașinile sunt strict controlate, se poate utiliza prima abordare. Însă pentru un mediu în care trebuie aprobate request-urile de la host-uri care nu sunt sub controlul unei organizații, trebuie să fie adoptată a treia abordare - utilizatorul trebuie să-și dovedească identitatea pentru fiecare serviciu dorit. Nu este suficient să se securizeze fizic host-ul, cineva în altă parte a rețelei, ar putea să se deghizeze în serverul dat.

Kerberos este o implementare care îndeplinește aceste cerințe. Atunci când utilizatorul se autentifică, din punctul său de vedere, această identificare inițială este suficientă pentru a-i dovedi identitatea tuturor serverelor din rețea necesare pe durata sesiunii de autentificare. Securitatea protocolului Kerberos se bazează pe securitatea serverelor de autentificare, dar nu și pe sistemul de unde se conectează utilizatorii, nici pe securitatea serverelor finale care vor fi utilizate. Serverul de autentificare oferă unui utilizator corect autentificat o modalitate de a-și dovedi identitatea serverelor din rețea.

Numele "Kerberos" are origini în mitologia greacă. În mitologia greacă, Kerberos (sau Cerberus în limba latină) era un monstru cu trei capete și un câine de pază care păzea poarta infernului, cunoscută sub numele de Poarta Hadesului sau Poarta Tartarului. În legendele grecești, Kerberos era considerat o ființă extrem de feroce și de temut, iar rolul său principal era să prevină ieșirea sufletelor din lumea de dincolo și să împiedice intrarea străinilor în această lume.

Alegerea numelui "Kerberos" pentru protocolul de securitate a fost influențată de conceptul de protejare a accesului și de păstrarea unei "porți" sau a unui punct de acces sigur în sistemele informatice. Ideea este că protocolul Kerberos servește ca un "câine de pază" pentru resursele și serviciile dintr-o rețea, asigurându-se că doar utilizatorii autentificați și autorizați au acces la acestea.

Kerberos a fost dezvoltat inițial pentru a permite utilizatorilor să se autentifice în rețelele locale fără a fi nevoie să introducă o parolă de fiecare dată când se conectează la un serviciu.

Versiunea 1

Prima versiune a Kerberos, numită Kerberos 1, a fost lansată în 1988. Această versiune a fost concepută pentru a fi folosită în rețelele locale mici și a utilizat o cheie partajată pentru a autentifica utilizatorii.

Versiunea 5

Versiunea 5 a Kerberos, numită Kerberos 5, a fost lansată în 1993. Această versiune a fost concepută pentru a fi folosită în rețele mai mari și a utilizat o infrastructură de cheie publică pentru a autentifica utilizatorii.

Popularitatea Kerberos

Kerberos a devenit rapid popular în rândul sistemelor de operare Unix și Linux. Protocolul a fost integrat în distribuțiile majore de Linux, cum ar fi Red Hat Enterprise Linux și Ubuntu.

Începând cu anul 2000, Kerberos a început să fie folosit și în sistemele de operare Windows. Microsoft a inclus suport pentru Kerberos în Windows 2000 Server.

Kerberos astăzi

Kerberos este astăzi unul dintre cele mai populare protocole de autentificare și autorizare. Este folosit pe scară largă în rețelele locale, rețelele la distanță și cloud computing.

Kerberos păstrează o bază de date a clienților săi și a cheilor lor private. Cheia privată este un număr mare cunoscut doar de Kerberos și de clientul respectiv, derivat prin procesul de hashing al parolei setate de client-ul respectiv. Serviciile de rețea care necesită autentificare se înregistrează la Kerberos, la fel și clienții care doresc să utilizeze acele servicii. Cheile private sunt negociate la înregistrare si servesc ca autentificare de lunga durata.

Datorită faptului că protocolul Kerberos cunoaște aceste chei private, poate crea mesaje care să ateste unui client că alt client este cu adevărat cine pretinde a fi. Kerberos generează, de asemenea, chei private temporare, numite chei de sesiune, care sunt date la doi clienți și nimănui altcuiva. O cheie de sesiune poate fi folosită pentru a cripta mesajele între două părți (client-client, client-service, service-service). Aceste chei private temporare nu au rolul doar pentru criptare ci, in lipsa lor, cele doua parti refuza comunicarea intre ele, deci are rol si de autentificare.

Kerberos oferă trei nivele distincte de protecție. De exemplu, unele aplicații solicită doar stabilirea autenticității la începutul unei conexiuni de rețea și pot presupune că mesajele ulterioare de la o anumită adresă de rețea provin de la părtea autentificată. Alte aplicații solicită autentificarea fiecărui mesaj. Pentru acestea, Kerberos oferă mesaje sigure. Totuși, un nivel mai înalt de securitate este furnizat de mesajele private, în care fiecare mesaj nu este doar autentificat, ci și criptat. Mesajele private sunt folosite, de exemplu, de serverul Kerberos însuși pentru a trimite parole peste rețea.

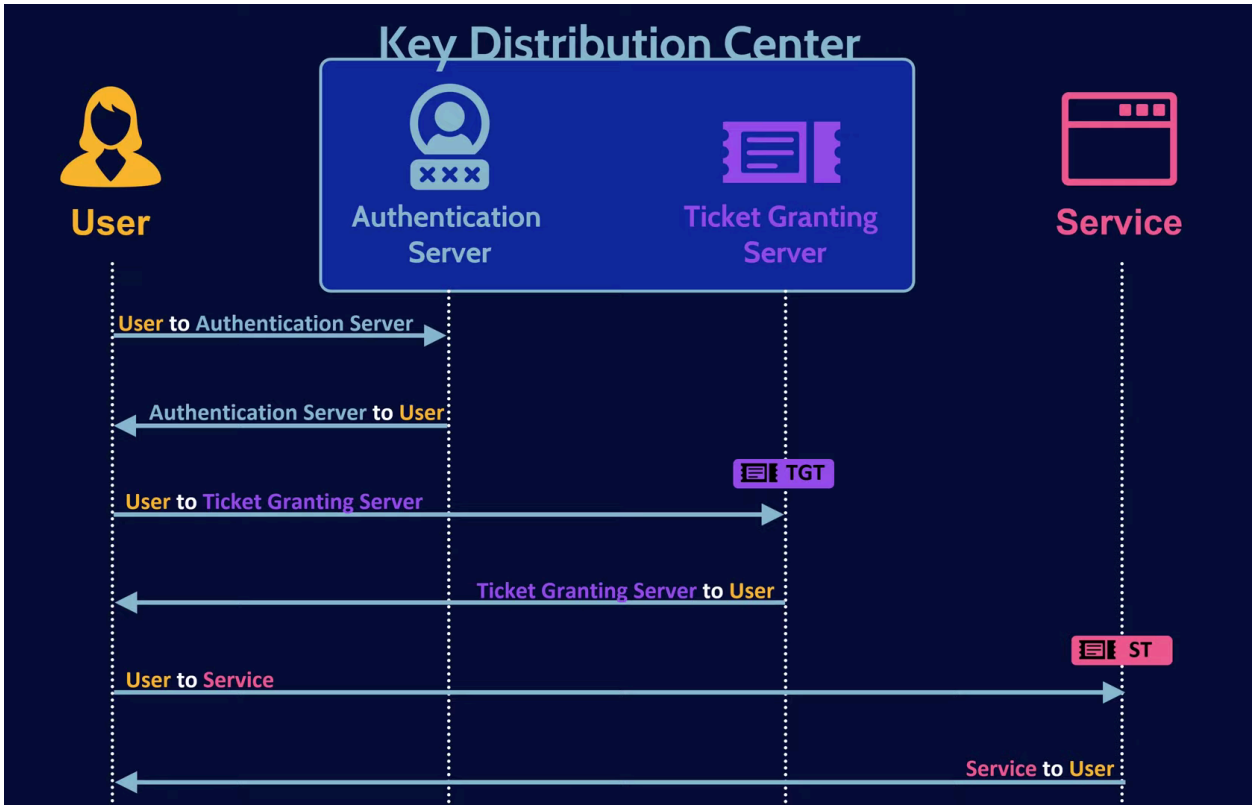
Pentru a sumariza aceste informații, Kerberos poate fi descris prin aceste fraze:

- Protocol care asigură acces securizat la servicii într-o rețea potențial nesigură.
- Parolele nu sunt trimise niciodată peste rețea
- Cheile de criptare nu sunt schimbate în mod direct
- Client-ul și serviciul se pot autentifica reciproc
- Multe organizații folosesc Kerberos ca bază pentru „single sign-on” (autentificare unică)

Pentru a înțelege cum funcționează protocolul Kerberos, este necesar să definim înainte niște termeni des utilizați:

- Kerberos realm: domeniul / grupul de sisteme asupra cărora Kerberos are autoritatea de a autentifica un utilizator pentru un serviciu.
- În cadrul unui Kerberos realm există:
    - Principals: o identitate unică (utilizatori sau servicii)
    - Client: proces care accesează un serviciu în numele unui utilizator; într-un realm pot exista mai mulți clienți – aceștia sunt utilizatorii care doresc să acceseze resurse.
    - Service: o resursă furnizată unui client, cum ar fi un server de fișiere sau o aplicație – pot exista mai multe servicii pe care un utilizator le poate accesa
    - KDC – Key Distribution Center – KDC-ul este „inima” protocolului Kerberos; acesta furnizează bilete și generează chei de sesiune temporare care permit unui utilizator să se autentifice în mod securizat la un serviciu; KDC stochează toate cheile secrete simetrice pentru utilizatori și servicii. În cadrul KDC există două servere:
        - Authentication Server: acesta confirmă că un utilizator cunoscut face o cerere de acces și emite „ticket granting tickets”

- Ticket Granting Server (Serverul de acordare a biletelor): acesta confirmă că un utilizator face o cerere de acces la un serviciu cunoscut și emite „service tickets”.



Protocolul Kerberos implică mai mulți pași principali pentru a permite autentificarea și autorizarea utilizatorilor într-o rețea securizată:

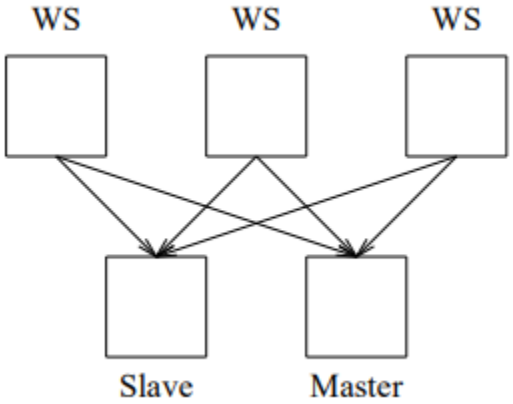
1. Autentificarea la KDC (Key Distribution Center):
   - Utilizatorul dorește să se autentifice la rețeaua securizată și solicită un bilet de autentificare (TGT - Ticket Granting Ticket).
   - KDC este un server central care gestionează autentificarea și autorizarea în sistemul Kerberos.
2. Obținerea TGT:
   - KDC verifică identitatea utilizatorului și generează un TGT criptografic, care conține informații despre utilizator și o cheie de sesiune.
   - Acest TGT este criptat cu o cheie secretă a KDC și trimis utilizatorului.

3. Obținerea unui bilet de serviciu (Service Ticket):
    - Utilizatorul dorește să acceseze un serviciu specific în rețea (de exemplu, un server de fișiere).
    - Utilizatorul folosește TGT-ul obținut pentru a solicita un bilet de serviciu pentru acel serviciu.
4. KDC generează un bilet de serviciu pentru utilizator, care conține informații despre serviciu și este criptat cu cheia de sesiune a serviciului.
    - Accesarea serviciului:
    - Utilizatorul trimite biletul de serviciu către serviciul dorit.
    - Serviciul decriptează biletul de serviciu folosind cheia sa de sesiune și verifică autenticitatea și autorizarea utilizatorului.
    - Dacă totul este corect, serviciul permite accesul la resursa sau serviciul solicitat.
5. Sesiunea de comunicare:
    - Utilizatorul și serviciul pot comunica acum într-o sesiune securizată, folosind cheia de sesiune stabilită.

Algoritmii de Criptare Suportați: Kerberos suportă o varietate de algoritmi de criptare, inclusiv DES, AES, și RC4. Versiunile mai recente încurajează folosirea AES datorită securității sale îmbunătățite. Criptografia asigură confidențialitatea și integritatea datelor transmise.

Managementul Cheilor: Kerberos utilizează un model centralizat de distribuție a cheilor prin KDC. Cheile simetrice sunt folosite pentru a cripta comunicațiile între clienți și servicii. Managementul eficient al cheilor implică reînnoirea periodică și distribuția sigură a acestora.

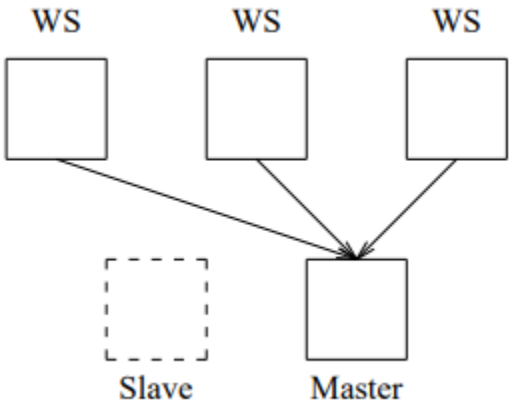
Procesele de Reînnoire a Tichetelor: Tichetele Kerberos au o durată de viață limitată, necesitând reînnoire pentru sesiuni prelungite. Procesul de reînnoire minimizează riscul compromiterii tichetelor și reduce necesitatea reautentificării frecvente de către utilizatori.



Baza de date Kerberos

Operatiile sunte executate de serviciul de autent pot rula atat pe masini master dar si slave.

Doar mașina principală Kerberos poate rula serverul KDBM, care este responsabil pentru gestionarea modificărilor la baza de date Kerberos. Copiile sclave ale bazei de date sunt numai pentru citire, iar modificările trebuie făcute direct în baza de date principală.



Serverul KDBM

Serverul KDBM acceptă cereri pentru a adăuga principali în baza de date sau pentru a schimba parolele principalelor existente. Acest serviciu este unic prin faptul că serviciul de emitere a tichetelor nu va emite tichete pentru el. În schimb, trebuie utilizat serviciul de autentificare însuși (același serviciu care este folosit pentru a obține un tichet de acordare a tichetelor). Scopul acestei abordări este de a solicita utilizatorului să introducă o parolă. Dacă nu ar fi așa, atunci dacă un utilizator și-ar lăsa stația de lucru nesupravegheată, un trecător ar putea să se apropie și să-i schimbe parola, ceea ce ar trebui prevenit. La fel, dacă un administrator și-ar lăsa stația de lucru nesupravegheată, un trecător ar putea schimba orice parolă din sistem.

Când serverul KDBM primește o cerere, o autorizează comparând numele principalului autentificat al solicitantului schimbării cu numele principalului țintă al cererii. Dacă acestea sunt identice, cererea este permisă. Dacă nu sunt identice, serverul KDBM consultă o listă de control

al accesului (stocată într-un fișier pe sistemul principal Kerberos). Dacă numele principalului solicitant este găsit în acest fișier, cererea este permisă, altfel este refuzată.

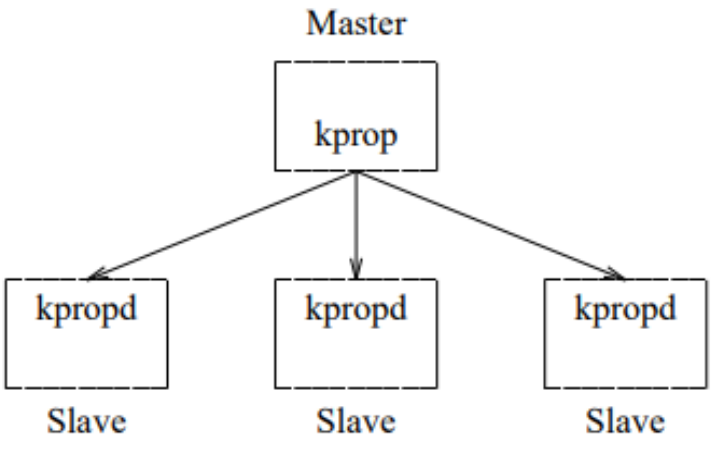
Prin convenție, numele cu o instanță NULL (instanța implicită) nu apar în fișierul listei de control al accesului; în schimb, se utilizează o instanță de admin. Prin urmare, pentru ca un utilizator să devină un administrator al Kerberos, trebuie creată o instanță de admin pentru acel nume de utilizator și adăugată la lista de control al accesului. Această convenție permite unui administrator să utilizeze o parolă diferită pentru administrarea Kerberos decât cea pe care ar folosi-o pentru autentificarea normală.

Toate cererile către programul KDBM, fie că sunt permise, fie că sunt refuzate, sunt înregistrate.

Kerberos folosește un sistem de replicare master-slave pentru a distribui baza de date de autentificare pe mai multe mașini. Mașina principală deține copia autorizată a bazei de date, în timp ce mașinile sclave mențin copii numai pentru citire. Această abordare îmbunătățește disponibilitatea și performanța, permițând continuarea autentificării chiar dacă mașina principală nu este disponibilă și distribuând sarcina solicitărilor de autentificare pe mai multe mașini.

Pentru a asigura consistența datelor, baza de date principală este copiată și trimisă mașinilor sclave la fiecare oră. Copierea este criptată folosind cheia bazei de date principale Kerberos, care este partajată între mașinile principale și sclave. La primirea copiei, mașina sclavă calculează un checksum al datelor și îl compară cu checksumul trimis de către master. Dacă checksumurile se potrivesc, mașina sclavă își actualizează baza de date cu noile informații.

Această schemă de replicare oferă un echilibru între disponibilitate, performanță și consistență a datelor în autentificarea Kerberos.



Vulnerabilități

Principalele vulnerabilități ale Kerberos includ atacurile de tip replay, unde un atacator interceptează și reutilizează mesaje autentificate, și atacurile prin forță brută asupra cheilor slabe. Kerberos poate fi de asemenea vulnerabil la atacuri de tip man-in-the-middle dacă nu se folosește criptografia pentru toate conexiunile. Mitigarea acestor riscuri implică utilizarea unor politici stricte de securitate, inclusiv actualizări regulate ale software-ului și a cheilor criptografice, precum și monitorizarea activităților suspecte în rețea.

Comparație cu alte protocoale de autentificare

Comparând Kerberos cu alte protocoale de autentificare, cum ar fi OAuth și SAML, Kerberos se distinge prin utilizarea criptografiei simetrice și a unui model bazat pe bilete pentru autentificarea mutuală între clienți și servicii într-un mediu închis, precum o rețea corporativă. OAuth se concentrează pe autorizarea accesului la resurse fără a transmite credențiale, fiind mai flexibil și adaptat aplicațiilor web și mobile. SAML este utilizat în principal pentru autentificarea și autorizarea între domenii diferite, oferind un mecanism robust pentru Single Sign-On (SSO) în aplicații enterprise. Kerberos oferă o soluție puternică pentru scenarii unde securitatea internă și autentificarea rapidă sunt critice, în timp ce OAuth și SAML sunt mai potrivite pentru integrarea și interoperabilitatea aplicațiilor web la scală largă.

Microsoft Active Directory (AD) este o soluție de gestionare a identității și accesului care utilizează Kerberos și LDAP (Lightweight Directory Access Protocol) în mod extensiv. În timp ce Kerberos se concentrează pe autentificarea mutuală într-un mediu închis, Microsoft AD extinde această funcționalitate pentru a include gestionarea centralizată a conturilor de utilizator, a drepturilor de acces și a altor informații de identitate într-o rețea. LDAP, pe de altă parte, este un protocol de acces la directoare, folosit pentru interogarea și actualizarea informațiilor de director. AD folosește LDAP pentru a organiza și accesa datele despre utilizatori și resurse într-un mod ierarhic. Astfel, în timp ce Kerberos se axează mai mult pe autentificarea securizată într-un context limitat, AD adaugă LDAP pentru a gestiona identitatea și accesul la nivel de

întreaga rețea, oferind un cadru mai amplu pentru administrarea identității într-un mediu corporativ.

Scalare

Pentru scalarea infrastructurii Kerberos în vederea suportării unui număr mare de utilizatori și tranzacții, este importantă implementarea unor soluții de distribuție a sarcinii și redundanță. Utilizarea mai multor servere KDC într-o configurație distribuită poate îmbunătăți performanța și disponibilitatea. De asemenea, monitorizarea performanței sistemului Kerberos, inclusiv timpul de răspuns al autentificării și utilizarea resurselor, este crucială pentru detectarea timpurie a problemelor și optimizarea sistemului. Strategii precum caching-ul tichetelor și optimizarea configurării rețelei pot ajuta, de asemenea, la îmbunătățirea performanței și scalabilității.