RoostGPT וסחואמ AWS-ב הסירפ - ומצעב Terraform תועצמאב

תמירע תא חראל ידכ RoostGPT יאמצע ופואב ,סיקוקז ונא סיאבה תיתשתה יבאשמל.

- סינותנ דסמ MySQL וא Postgres
- תודועת SSL וימודו DNS
- שדחמ הינפה רובע oAuth סושייל סירושקה DNS תרוצתו דוס ,חוקל ההזמ
- תשרו וניע בושחמ יבאשמ תרדגה רזרוצל וניעב סינותנ זכרמ לש תונימז רוזאו IP CIDR חווט יוהיז

Terraform טפירקס תועצמאב וצקוי סיאבה סיבאשמה

- VPC רעשו תומיאתמ תויטרפו תוירוביצ תותשר-תתו NAT
- סיוולנ וסחא יעצמאו Ubuntu Compute (EC2) יעפומ
- דעי תוצובקו סימושיי לש סיסמוע וזאמ

- 1. הדובעה תליחת
- 2. קפס תרדגה OAuth
- 3. סינותנ דסמ תרדגה
- 4. המרופארט ינתשמ
- 5. RoostGPT לש הרקבה חטשמ לש הקוזחת/גורדש

1. הדובעה תליחת

Roost תקפסמ לש סיטפירקס Terraform לש הרוצתה תא עובקלו ליעפהל ידכ תמרופטלפ לש RoostGPT תולקב. ולהל תסירפל סיבלשה Roost ב-AWS תועצמאב Terraform.

ההובג המרב הרוטקטיכרא

AWS ונעב סיאבה סיביכרה תא סירצוי Roost Terraform לש סיטפירקס

RoostGPT-architecture-multiple-ec2.jpg

תבותכב תיביטקארטניא המרגאיד https://docs.roost.ai/arch

סדק תושירד

- terraform לש סיטפירקס תלעפהל תולעפומ תוינידמ / להנמ תואשרה סע שמתשמ וובשח
- רֹוזֵא
- 53לולסמ_חראמ_רוזא_ההזמ
- ec2_ami (22.04 ימא'ג וטנובוא רובע)
- dns_ינוגרא
- ip_block_vpc (VPC CIDR סקוי ובש Roost)
- okta_client_id סיאתמ תומיא קפס וא (אבה ףיעסב ונייע אנא)
- הרבחה סש

Terraform לש סיטפירקסה תא דרוה

```
curl -LO https://github.com/roost-io/roost-support/raw/refs/heads/master/terraform-ec2.zip
```

2. קפס תרדגה OAuth

Roost רמות ינונגנמב תומיא ינוש יפכ ויוצש וללה

1. הטקוא
2. לגוג
3. ADFS רו'ת טפוסורקימ

OKTA תומיא חוקל תרדגה

- OKTA ובשחל סנכיה להנמ תואשרה סע רלש (*Okta ובשח רל ויא מא, סייק פדב משריה* חתפמ | תיבה Okta)
- סימושיי -> סימושיי לא רובע, ילאמשה טווינה טירפתמ.
- אבה לע ץחל וכמ רחאל, טנרטניא סושיי ← OIDC - OpenID Connect ← היצקילפא תייצרגטניא רוצ רחב
- תא ואלמ **היצקילפאל סיאתמה היצרגטניאה סש,** וגולה תא ולעה.
- פסוה **הסינכ לש שדחמ הינפהל URI תובותכ**
  - https://<סש_DNS>/תורבחתה
- תרקובמ השיג → תומישמ ךרד סישמתשמל השיג רשפא
  - סלוכל השיג רשפא וא סישמתשמה תוצובק תא רחב
- (הטמל הרוצתב רשמהב רכב ךרוצ שי) חוקלה דוס תאו Okta לש חוקלה ההזמ תא רמצעל סושרו רומש
- החטבא לא רובע, ילאמשה טווינה טירפתמ -> API
- לדחמ תרירבכ רדגומה תואשרהה תרש רובע **קיפנמה לש URI-ה** תא רמצעל סושר
  - ומכ והשמ https://{your_domain}.okta.com/oauth2/default

לגוג תומיא חוקל תרדגה

- לגוג יחתפמ | טנרטניא ירתאל לגוגמ הסינכ | רלש טנרטניאה תייצקילפאב לגוגמ הסינכ בוליש
- לא רבחתה https://console.cloud.google.com/apis/credentials
- טנרטניא תייצקילפאכ סושיי גוסו OAuth חוקל רחב, סירושיא רוצ
- כ השרומ JavaScript רוקמ פסוה
  - https://<סש_DNS>

- שדחמ הינפהל תושרומ URI תובותכ פסוה
  - https://<סש_DNS>/תורבחתה
  - https://<סש_DNS>/api/auth/redirect/google
- ה-JSON ץבוק תא דרוה

- (הטמל הרוצתב רשמהב שרדנ) חוקלה דוס תאו לגוג לש חוקלה ההזמ תא רמצעל סושר

Azure ADFS תומיא חוקל תרדגה

Roost 0Auth2 Setup - Windows Server 2016/2019 - ADFS 4.0

1. **AD FS לוהינ** > **סילכ** רחב **,לחתה** טירפתמ **סיתרשה להנמ** תא חתפ
2. ממ **AD FS לוהינ** רסמנ , לא רובע **AD FS ← סימושיי תוצובק**
3. תינמיה תינולחב **סימושיי תצובק יפסוה** לע ץחל

1. אלמ **סש** (**Roost**) סימושייה תצובק רובע
2. **אבה** לע ץחלו **יטנרטניא API-ל שגינש תרש סושיי לש טנרטניא יפדפד** רחב
3. הנתשמה `AZURE_ADFS_CLIENT_ID` לש ךרעה היהי הז . **חוקלה ההזמ** לש ךרעל בל ומיש
4. אבה לע וכמ רחאל ,יפסוה לע וצחלו (https://<DNS_NAME>/login) **הינפהל URI-ה תבותכ** תא ואלמ
5. **יתושמ דוס רוצ** הביתה תא ומס
6. שמתשה וצחלב **חולל קתעה** לש ךרעה היהי הז .דוסה תא רזחאל ידכ `AZURE_ADFS_CLIENT_SECRET` הנתשמה. **אבה** לע וצחל
7. ה-Web API (ההז ל-RedirectUri - https://<DNS_NAME>/login) לע ץחלו **יפסוה,** רחאל וכמ **.אבה לע** ההזמ תא וזה
8. **אבה** לע ץחלו **סלוכל רשפא** ללכ ךרדב ,תוינידמ רחב , **השיג תרקב תוינידמ** רסמב
9. ה- **openid לש** יפקיהה **אבה** לע ץחלו , **סושיי תואשרה תרדגה** רסמב
10. **אבה לע וצחלו תורדגהה תא רוקס**
11. ב- ADFS . תעכ המושר ונלש היצקילפאה . **רוגס** לע הציחל ידי לע יפשאה תא רוגס

1. סושייה רובע **תועיבתה תא רידגהל** ונילע ,תעכ

1. ונרצי התע הזש סימושייה תצובק רובע.
2. **הכירע** לע ץחלו (**Roost - Web API**) **טנרטניאה סושיי** ךרע תא רחב
3. **ללכ יפסוה** וצחל לע ץחל , **הקפנה לש היצמרופסנרט יללכ** הייסיטרכב
4. **אבה** לע ץחלו **תועיבתכ LDAP ינייפאמ חלש** רחב
5. ללכל סש וק (**Roost Claims**) תא רחבו **Active Directory** סינייפאמה רגאמכ.
6. תנוכת) תואבה תועיבתה תא רדגה תעכ **תאצוי העיבת גוס => LDAP**):

1. ל"אוד תבותכ => ל"אוד תובותכ
2. יטרפ סש => יטרפ סש
3. החפשמ סש => החפשמ סש
4. וובשח סש SAM => וובשח סש Windows
5. ישאר שמתשמ סש => UPN

1. תועיבתה תא רומשל ידכ **סויס לע** ץחל
2. תורדגהה תא רומשל ידכ סימעפ רפסמ **רושיא** לע ץחל .יפסונ ללכה תא תוארל רומא התא תעכ.

1. הביבס ינתשמכ סיאבה סיכרעה תשולש תא ונעבק. המלשוה הנקתהה תעכ:

1. `AZURE_ADFS_CLIENT_ISSUER` - מוחת תרש לש ADFS (https://adfs.contoso.com)
2. `AZURE_ADFS_CLIENT_ID` - תרש מושיי לש חוקל ההזמ
3. `AZURE_ADFS_CLIENT_SECRET` - חולל ונקתעהש חוקלה דוס

`AZURE_ADFS_CLIENT_SECRET` תא הנתשמה שמתשהל הצור רניא מא ,חוקלה דוסב שמתשהל הצור רניא מא ריבעהו ירוקמ מושיי ךסוה.

3. מינותנ דסמ תרדגה

Roost וסחאמ תא סוטטס תמירז עדימו GPT לש הדובעה תמירז יטנוולר רחא דסמב מינותנה. Roost רמות ב-MySQL, Postgres ו-Amazon Aurora DB. ש-RoostGPT לעפי ידכ שרדנ מינותנ דסמ לכ.

תרדגהל מיבלשה ולהל RDS ב-AWS

MySQL וא (MySQL-ל מאות) הרורוא וזמא

1. רחב RDS
2. מינותנ דסמ רוצ רחב
3. רחב "הלק הריצי" רובע "Amazon Aurora תומיאת עם MYSQL" וא "MySQL"
4. רושימ יעפומ לש החטבאה תצובקל TCP 3306 תאיציל השיג רשפאל ידכ RDS לש החטבאה תצובק תא הנש דבלב הרקבה.
5. רכב רזוצ שי) בתוכה עפומ לש מינותנה דסמ לש המסיסהו שמתשמה, הצקה תדוקנ תא רמצעל סושר וזלהלש הרוצתב רשמהב)

תכרעמ להנמ לש תורבחתהב שומישמ ענמיהו הביתכו האירק תואשרה סע שדח שמתשמ רוצ.

```
# Sample command to create a user using MySQL CLI
# Provide password on prompt

mysql -h <SQL Host URL> -u <root|master|admin> -p
```

```
CREATE USER 'Roost'@'%' identified WITH mysql_native_password by 'Roost#123';
CREATE DATABASE roostio;
GRANT ALL on roostio.* to 'Roost'@'%';

# Execute the Roost Schema file, if available
\. /var/tmp/Roost/db/roost.sql
```

PostgreSQL וא (PostgreSQL-ל מאות) הרורוא וזמא

1. רחב RDS

2. סינותנ דסמ רוצ רחב
3. רחב "הלק הריצי" רובע "Amazon Aurora תומיאת סע PostgreSQL" וא "PostgreSQL"
4. רושימ יעפומ לש החטבאה תצובקל TCP 5432 תאיציל השיג רשפאל ידכ RDS לש החטבאה תצובק תא הנש דבלב הרקבה.
5. בתוכה עפומ לש סינותנה דסמ לש המסיסהו שמתשמה, הצקה תדוקנ תא רמצעל סושר רכב רזוצ שי) ולהלש הרוצתב רשמהב)
6. תכרעמ להנמ לש תורבחתהב שומישמ ענמיהו הביתכו האירק תואשרה סע שדח שמתשמ רוצ.

```
psql "host=<PG Host URL> user=<admin> dbname=postgres port=5432 sslmode=require"
```

```
CREATE DATABASE roostio;                                -- creates app database [5]
CREATE USER roost WITH PASSWORD 'Roost#123';            -- creates login role [3]
GRANT ALL PRIVILEGES ON DATABASE roostio TO roost;      -- DB-level grant [4]

-- Connect to the new DB (reconnect as admin or roost), then set schema privileges
\c roostio
GRANT USAGE ON SCHEMA public TO roost;
GRANT ALL ON ALL TABLES IN SCHEMA public TO roost;
GRANT USAGE ON ALL SEQUENCES IN SCHEMA public TO roost;
ALTER DEFAULT PRIVILEGES IN SCHEMA public
  GRANT ALL ON TABLES TO roost;
ALTER DEFAULT PRIVILEGES IN SCHEMA public
  GRANT USAGE ON SEQUENCES TO roost;

-- Execute the Roost Schema file, if available
\i /var/tmp/Roost/db/roost.sql
```

4. המרופארט ינתשמ

תא בלשל ידכ terraform יצבק תונשל ידכ סיאבה סיבלשה תא ועצב אנא

- קתעה `terraform.tfvars.original` כ `terraform.tfvars`
- סיאבה סיטרפה תא ואלמ (וקפוס רבכ המגוד יכרע)

```
enterprise_dns = "subdomain.domain.com"
admin_email = "comma separated list of emails"
enterprise_email_domain = "email-domain.com"
company = ""
license_key = ""
roost_jwt_token = "32-character-secure-long-secret"
roost_version = "v1.1.17"

az1_suffix = "b"
az2_suffix = "c"
certificate_arn = "arn:aws:acm:region:account:certificate/cert-id"
ec2_ami = "ami-023a307f3d27ea427"
region = "region"
ip_block_vpc="172.32.255.192"
route53_hosted_zone_id = ""
key_pair = "roost-ssh"

azure_tenant_id = ""
azure_client_id = ""
azure_client_secret = ""
okta_client_id = "your client id"
okta_client_secret = "your client secret"
okta_issuer = "https://account.okta.com/oauth2/default"

is_own_mysql = false
mysql_db_name = "roostio"
mysql_host = "mysqldb_host_url"
mysql_password = "Roost#123"
mysql_port = 3306
mysql_root_password = "Admin#123"
```

```
mysql_username = "Roost"
```

Terraform תורדגה ינתשמ

Field	Values	Description
roost_version	"v1.1.17"	
license_key		
prefix	"terraform-gpt"	
region	"us-west-1"	
az1_suffix	"b"	
az2_suffix	"c"	
deletion_protection	false	
route53_hosted_zone_id		
enterprise_dns	"roostgpt.example.com"	
enterprise_ssl_certificate_path	"/var/tmp/Roost/certs/server.cer"	
enterprise_ssl_certificate_key_path	"/var/tmp/Roost/certs/server.key"	
certificate_arn	""	
ec2_ami	"ami-03df6dea56f8aa618"	
key_pair	"roost-gpt-keypair"	
generate_key_pair	true	
device_name	"sdh"	
ip_block_vpc	"172.32.255.192"	
instance_type_controlplane	"c5a.2xlarge"	
instance_type_jumphost	"t3.micro"	

disk_roostgpt	150	
disk_jumphost	150	
disk_controlplane	150	
google_client_id		
google_client_secret		
github_client_id		
github_client_secret		
linkedin_client_id		
linkedin_client_secret		
azure_tenant_id		
azure_client_id		
azure_client_secret		
okta_client_id	"0oa4bweaxcqn2sfTu5d7"	
okta_client_secret	"D5oRtWXUWcl9gp1312dVtuSoumU4vrECO4wSsqAO"	
okta_issuer		
roost_jwt_token		
company		
company_logo	"https://roost.ai/hubfs/logos/Roost.ai-logo-gold.svg"	
enterprise_email_domain	"example.com"	
admin_email	"admin@email"	
admin_email_pass	""	
senders_email	"sender@email"	

is_own_mysql	false	
db_type	"mysql"	
mysql_host	"mysqldb_host_url"	
mysql_password	"Roost#123"	
mysql_username	"Roost"	
mysql_port	3306	
mysql_db_name	"roostio"	
mysql_root_password	"Admin#123"	
senders_email_pass		
email_smtp_host		

5. חטשמ לש הקוזחת/גורדש RoostGPT לש הרקבה

תושיגהמ תחא לכב שמתשהל לוכי תיתשתה סדנהמ RoostGPT. תינסחמ גורדש וא וונערל תונימז תויורשפא רפסמ ונשי וללה.

א. RoostGPT טפירקסב שומיש תסרג גורדשל Terraform

המיאתמה Roost תסרג תא ךקשל ידכ "terraform.tfvars" -ב Terraform ינתשמ וכדע

הֶדָשׂ	סיכרע
טסורה_תסרג	הסרג 1.1.17

תואבה תודוקפה תא לעפה:

```
terraform apply
```

ב. הרקבה חטשמ וונערל Terraform טפירקסב שומיש (הרוצת יוניש אלל)

תואבה תודוקפה תא לעפה

```
terraform apply --replace="null_resource.provision-controlplane-system" --replace="null_resource.provision-roostgpt-server" --replace="null_resource.run-controlplane-services"
```

ג. הרקבה רושימב עפומ עוציבל SSH-ב שומיש

לש הרקבה חטשמ RoostGPT זירמ לש רוביח טפירקס docker וחינו וכדעל תא לכ עציהה תועצמאב סיבלשה סיאבה.

- וטנובוא שמתשמכ רלש תיתשתה לש וויטסבה תכרעמל SSH תורבחתה
- הסרג תפלחה רחאל) המיאתמה Roost תסרג סע אבה עטקה תא עצב 1.1.17)

```
ssh cp "ROOST_VER='v1.1.17' /var/tmp/Roost/bin/roost-enterprise.sh -c /var/tmp/Roost/config.json -i roostai"
```