



## راهنمای نصب و بهره‌برداری از کنسول مدیریت BIND

### ۱. مقدمه و معرفی سیستم

سرویس **BIND (Berkeley Internet Name Domain)** یکی از پرستفاده‌ترین نرم‌افزارهای DNS در زیرساخت‌های اینترنت است. با این حال، مدیریت دستی فایل‌های پیکربندی آن همواره با ریسک خطای انسانی همراه است. این کنسول مدیریتی که با زبان **Go** توسعه یافته است، یک رابط کاربری برای مدیریت زون‌ها، لیست‌های دسترسی (ACL) و امنیت DNS فراهم می‌کند.

### ویژگی‌های کلیدی پروژه:

- مدیریت متمرکز فایل‌های `named.conf`.
- پشتیبانی از پروتکل‌های امن **DoT** و **DoH**.
- مانیتورینگ زنده کوئری‌های DNS.
- رابط کاربری دو زبانه (فارسی و انگلیسی).

### ۲. پیش‌نیازهای سیستم

برای اجرای صحیح اسکریپت نصب و عملکرد کنسول، سیستم شما باید واجد شرایط زیر باشد:

- سیستم عامل: **Ubuntu 24.04**
- دسترسی: سطح دسترسی **Root** برای ویرایش فایل‌های سیستم و مدیریت سرویس‌ها.
- پورت‌های آزاد: پورت ۸۰ برای پنل وب و پورت ۵۳ برای سرویس DNS.
- نام سرویس در OS: `bind-admin`

### ۳. فرآیند نصب (Installation)

نصب سیستم از طریق فایل `bind-admin.sh` انجام می‌شود. این اسکریپت مراحل زیر را به صورت خودکار طی می‌کند:

۱. آماده‌سازی: غیرفعال کردن سرویس‌های مزاحم مانند `systemd-resolved`.
  ۲. نصب پکیج‌ها: نصب `BIND9`، ابزارهای DNS و زبان `Go`.
  ۳. پیکربندی لاگ: ایجاد فایل‌های لاگ و تنظیم دسترسی‌های `AppArmor`.
  ۴. تعیین هویت: دریافت نام کاربری و رمز عبور مدیر ذخیره به صورت هش (SHA-256).
- جهت نصب ابتدا فایل را داخل OS قرار داده سپس دستورات زیر را اجرا می‌کنید:

```
chmod +x bind-admin.sh
```

```
./bind-admin.sh
```

در صورت استفاده از `DOH`، `DOT` به فایل‌های `privkey.pem`، `fullchain.pem` نیاز داریم.



```

> Step 1: System Preparation
  → No previous installation found
  ✓ Installation directories created

> Step 2: Package Installation
  ✓ BIND9 already installed
  ✓ BIND9 service enabled
  ✓ Golang already installed

> Step 3: Permissions & Logging Configuration
  ✓ Log permissions configured

> Step 4: Admin Credentials Setup
  Username (default: admin):
  ✓ Username set to: admin
  Password:
  ✓ Password configured

> Step 5: Network Configuration
  Configure Go Proxy (Nexus)? (y/n): y
  Nexus URL (leave empty to skip): https://nexus.monsef.local/repository/go-proxy/
  ✓ Go Proxy configured

> Step 6: DNS over TLS/HTTPS Configuration
  Enable DNS over TLS (port 853) & HTTPS (port 443)? (y/n): y
  Certificate path (fullchain.pem): /root/fullchain.pem
  Private key path (privkey.pem): /root/privkey.pem
  ✓ TLS/DoH enabled

> Step 7: AppArmor Configuration
  ✓ AppArmor rules applied

> Step 8: Backend Application Generation
  ✓ Backend code generated
  ✓ Professional stylesheet generated
  ✓ All templates generated
  ✓ Logo created (You can replace it at /opt/bind-admin/assets/img/logo.svg)

> Step 9: Application Compilation
  → Compiling Go application...
  ✓ Compilation successful

> Step 10: Service Configuration
  ✓ Service enabled and started

Installation Complete


Panel URL:    http://192.168.1.20
Username:    admin
Password:    [as configured]

Check service status: systemctl status bind-admin
```



#### ۴. ورود به سیستم و داشبورد


پس از نصب، پنل از طریق آدرس IP سرور و پورت ۸۰ در دسترس است.



### BIND Admin Panel

Sign In

- **صفحه لاگین:** امنیت ورود توسط کوکی‌های نشست (Session Cookies) تامین می‌شود.
- **داشبورد:** در این بخش وضعیت فعال بودن سرویس BIND نمایش داده شده و امکان ریستارت سرویس یا پاکسازی کش (Flush Cache) وجود دارد.



**BIND Admin**

Dashboard

Live Monitor

Access Lists

Zones

Global Settings

Dig Tools

FA

EN

Logout

## DNS Admin Panel

Flush Cache

Status:

Active

Hide Log

Restart Service

```

• named.service - BIND Domain Name Server
  Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
  Active: active (running) since Sun 2026-01-04 11:49:02 +0330; 56min ago
  Docs: man:named(8)
  Process: 12035 ExecReload=/usr/sbin/rndc reload [code=exited, status=0/SUCCESS]
  Main PID: 12595 (named)
  Status: "running"
  Tasks: 20 (limit: 9435)
  Memory: 44.3M (peak: 47.7M)
  CPU: 131ms
  CGroup: /system.slice/named.service
          └─12595 /usr/sbin/named -f -u bind

Jan 04 11:49:03 dns-cache named[12595]: reloading configuration succeeded
Jan 04 11:49:03 dns-cache named[12595]: resolver priming query complete: operation canceled
Jan 04 11:49:03 dns-cache named[12595]: reloading zones succeeded
Jan 04 11:49:03 dns-cache named[12595]: all zones loaded
Jan 04 11:49:03 dns-cache named[12595]: running
Jan 04 11:49:03 dns-cache rndc[12035]: server reload successful
Jan 04 11:49:03 dns-cache systemd[1]: Reloaded named.service - BIND Domain Name Server.
Jan 04 11:49:03 dns-cache named[12595]: managed-keys-zone: Unable to fetch DNSKEY set '': shutting down

```



## ۵. مدیریت لیست‌های دسترسی (ACL)

این بخش به شما اجازه می‌دهد گروه‌های IP معتمد را تحت عنوان trusted-lan تعریف کنید. این تنظیمات به صورت خودکار در فایل `/etc/bind/named.conf.acls` ذخیره می‌شوند.

- افزودن گروه: امکان دسته‌بندی IP ها برای مدیریت آسان‌تر.
- ویرایش و حذف: اعمال تغییرات آنی در لیست‌های دسترسی.

## ۶. مدیریت زون‌ها (Zone Manager)

شما می‌توانید دامنه‌های مورد نظر خود را تعریف کرده و آن‌ها را به Forwarder های مشخصی ارجاع دهید. این تغییرات در فایل `named.conf.web-zones` مدیریت می‌شوند.

- Forward Zones: تعریف دامنه و مشخص کردن IP سرورهای مقصد.



## ۷. مانیتورینگ و امنیت پیشرفته

### مانیتورینگ زنده (Live Monitor)

این کنسول قابلیت نمایش لحظه‌ای درخواست‌های DNS را دارد. شما می‌توانید مشاهده کنید که کدام کلاینت در چه زمانی چه دامنه‌ای را درخواست کرده است.

### امنیت (DoT / DoH)

در صورت ارائه گواهی‌های SSL، اسکریپت نصب پروتکل‌های **DNS over TLS** (پورت ۸۵۳) و **DNS over HTTPS** (پورت ۴۴۳) را فعال می‌کند.

**BIND Admin**

Dashboard

**Live Monitor**

Access Lists

Zones

Global Settings

Dig Tools

FA EN

Logout

**Live Query Monitor**

Real-time logging

Logging: **OFF**

Time	Client IP	Domain	Type
04-Jan-2026 12:56:31	127.0.0.1	youtube.com	A
04-Jan-2026 12:56:26	127.0.0.1	yahoo.com	A
04-Jan-2026 12:56:22	127.0.0.1	facebook.com	A
04-Jan-2026 12:56:18	127.0.0.1	google.com	A
04-Jan-2026 11:38:42	127.0.0.1	google.com	A



## ۸. تنظیمات کلی (Global Settings)

این بخش برای مدیریت رفتار عمومی سرور DNS در مواجهه با دامنه‌هایی است که در زون‌های داخلی تعریف نشده‌اند. (Recursive Queries)

### وظایف اصلی این بخش:

- مدیریت Forwarders: تعیین سرورهای DNS بالادستی (مانند ۸.۸.۸.۸ یا ۱.۱.۱.۱) برای پاسخگویی به درخواست‌های اینترنتی.
- پیکربندی فایل Options: تغییرات این بخش مستقیماً در فایل `/etc/bind/named.conf.options` اعمال می‌شود.
- حالت Forward Only: با ذخیره این تنظیمات، سرور به گونه‌ای پیکربندی می‌شود که فقط از فورواردرهای تعیین شده استفاده کند.

### نحوه استفاده:

۱. آدرس‌های IP سرورهای DNS مورد نظر خود را در کادر مربوطه وارد کنید.
۲. آدرس‌ها را با استفاده از "کاما" (,) از هم جدا کنید.
۳. پس از ذخیره، کنسول به طور خودکار صحت ساختار (Syntax) را بررسی کرده و سرویس BIND را بازنشانی (Reload) می‌کند.



## ۹. ابزارهای عیب‌یابی (Dig Tools)

داخل کنسول ابزاری برای تست DNS تعبیه شده است که از دستورات dig و kdi استفاده می‌کند. شما می‌توانید رکوردها را بر بستر UDP ، DoH یا DoT تست کنید و نتایج را مشاهده نمایید.

The screenshot shows the BIND Admin web interface. On the left is a sidebar with navigation links: Dashboard, Live Monitor, Access Lists, Zones, Global Settings, and Dig Tools (highlighted). The main content area is titled 'DNS Test'. It contains a form with three fields: 'Domain' (google.com), 'Type' (A), and 'Protocol' (UDP). Below the form is a 'Run' button. Under the 'Results' section, there are two panels: 'Local BIND' and 'Global Fwd'. Both panels show the output of a DNS query for google.com, including query time, server address, and response details.

در صورت استفاده از zoning هنگام تست ابتدا از خود سرور سپس از Forwarder های آن zone رکوئست داده شده و نمایش داده می‌دهد.

## ۱۰. نگهداری و فایل‌های سیستم

برای مدیران سیستم، لیست فایل‌های کلیدی ایجاد شده توسط کنسول به شرح زیر است:

- `/opt/bind-admin` : محل قرارگیری فایل‌های اجرایی و قالب‌ها.
- `/etc/bind/named.conf.options` : تنظیمات اصلی و فوروارددهای کلی.
- `/var/log/bind/queries.log` : محل ذخیره لاگ درخواست‌ها.

## ۱۱. عیب‌یابی و نکات کلیدی (Troubleshooting & Best Practices)

برای حفظ پایداری سرویس و بهره‌وری بهینه از کنسول مدیریتی، توجه به نکات زیر الزامی است:

- **الزام تعریف Forwarder در تنظیمات کلی:** در بخش **Global Settings**، همواره باید حداقل یک آدرس IP برای **Forwarder** تعریف شده باشد. در صورت خالی بودن این بخش، سرویس BIND در تحلیل نام دامنه‌های خارجی با مشکل مواجه شده و ممکن است به هیچ درخواستی پاسخ ندهد.
- **اعمال خودکار تغییرات (Auto-Reload):** برخلاف مدیریت سنتی در محیط خط فرمان (CLI)، در این کنسول پس از انجام هرگونه تغییر در تنظیمات (مانند افزودن زون یا ACL، نیازی به ریستارت دستی سرویس نیست. سیستم به طور هوشمند و در پس‌زمینه (Background)، پیکربندی‌ها را بازنشانی کرده و تغییرات را اعمال می‌کند.
- **مدیریت منابع در مانیتورینگ زنده (Live Monitor):** قابلیت **Live Monitor** به دلیل ثبت و تحلیل لحظه‌ای کوئری‌ها، بار پردازشی (Compute) و عملیات ورودی/خروجی (IOPS) نسبتاً بالایی اشغال می‌کند. لذا توصیه می‌شود این قابلیت را فقط در زمان‌های عیب‌یابی یا پیگیری‌های خاص در وضعیت **ON** قرار دهید و در سایر موارد برای حفظ کارایی سرور، آن را **OFF** نگه دارید.
- **بازایی قابلیت مانیتورینگ:** چنانچه در بخش مانیتورینگ زنده، لاگ‌ها به درستی نمایش داده نمی‌شوند یا متوقف شده‌اند، ابتدا یک بار سرویس BIND را از طریق بخش **Dashboard** ریستارت نمایید تا دسترسی‌های فایل لاگ و فرایندهای سیستم مجدداً تنظیم شوند.