

راهنمای فنی Safetica

مدیریت نگهداری، پشتیبان‌گیری و کنترل آپلود فایل

بر اساس: Safetica Complete Documentation v۱۰

موضوع	جزئیات
نوع سند	راهنمای فنی داخلی
محصول	Safetica ONE ۱۰.X
زبان	فارسی
موضوعات	Maintenance / Backup / DLP Policy

۱. بخش Maintenance — ساختار کلی

بخش Maintenance در کنسول Safetica، مرکز مدیریت کل زیرساخت امنیتی سازمان است. از این بخش می‌توان دیتابیس را مدیریت کرد، بکاپ گرفت، کاربران ادمین تعریف نمود، آپدیت‌ها را کنترل کرد و اطلاعات Debug جمع‌آوری کرد.

مسیر دسترسی: [Console](#) → [Maintenance](#) → [Database management](#)

۲. ساختار دیتابیس Safetica

برای درک صحیح فرآیند بکاپ، معماری دیتابیس Safetica باید شناخته شود. هر سرور به سه دیتابیس مستقل روی SQL Server نیاز دارد:

ردیف	نام دیتابیس	محتوا
۱ — دیتابیس تنظیمات	safetica_data	تنظیمات، پالیسی‌های DLP، کاربران، گروه‌ها
۲ — دیتابیس رکوردها	safetica_data (Records)	لاگ‌های فعالیت کاربران، رویدادهای فایل و شبکه
۳ — دیتابیس دسته‌بندی‌ها	safetica_categories	دسته‌بندی اپ‌ها، وب‌سایت‌ها، انواع فایل

⚠ هر سرور Safetica دیتابیس مستقل خود را دارد. در محیط‌های چند سروره، بکاپ باید برای هر سرور به‌طور جداگانه انجام شود.

۳. تب Tasks — مدیریت وظایف دیتابیس

مسیر: [Maintenance](#) → [Database management](#) → [Tasks](#)

در این بخش وظایفی برای مدیریت داده‌های ذخیره‌شده در دیتابیس تعریف می‌شود. با کلیک روی New archiving task یک task جدید ایجاد می‌شود.

۳-۱. انواع Task

نوع عملیات	توضیح	کاربرد
Backup	فقط بکاپ — داده‌های اصلی حذف نمی‌شوند	آرشیو لاگ‌ها برای مراجعه بعدی

خروج لاگ‌های قدیمی از دیتابیس عملیاتی	بکاپ + حذف داده‌های اصلی	Backup and Delete
پاکسازی دیتابیس بدون آرشیو	فقط حذف — بدون ایجاد بکاپ	Delete

۳-۲. پارامترهای Task

زمان‌بندی (Repeat Task)

- هر هفته
- هر ۱۴ روز
- هر ماه
- هر سه ماه

تنظیمات آرشیو

- Archive name: نام فایل بکاپ — نباید شامل کاراکترهای غیرمجاز مانند فاصله باشد
- Archive directory: مسیر ذخیره فایل بکاپ روی سرور SQL — این مسیر باید از قبل وجود داشته باشد

بازه زمانی لاگ‌ها

- From-To: بازه زمانی مشخص — مناسب برای task‌های یک‌بار اجرا
- Log older than: فقط لاگ‌های قدیمی‌تر از تاریخ مشخص — مناسب برای task‌های تکراری

اجرا و اولویت‌بندی

- Schedule execution at: زمان دقیق اجرا — باید خارج از بازه رکوردهای پردازش‌شده باشد
- Automatic replanning: در صورت تعارض زمانی، task به اولین زمان آزاد منتقل می‌شود
- Selected objects: کاربران، کامپیوترها یا گروه‌هایی که task شامل آن‌ها می‌شود

۳-۳. ستون‌های Records در Task

- Date and Time: تاریخ و زمان اجرا
- User Name: نام حساب ادمین + نام کامپیوتر
- Task Name: نام وظیفه اجراشده
- Archive Directory: مسیر ذخیره آرشیو
- Type of Task: نوع عملیات
- Details: جزئیات با کلیک روی دکمه Details

۴. تب Archives — مدیریت آرشیوها

مسیر: Maintenance → Database management → Archives

در این بخش آرشیوهای ایجادشده قبلی را می‌توان به سرور متصل کرد و محتوای آنها را در کنسول مشاهده نمود.

۴-۱. وارد کردن آرشیو (Import Archive)

۱. مسیر آرشیو را در فیلد مربوطه وارد کنید
۲. سرور هدف را انتخاب کنید
۳. روی دکمه Import archive کلیک کنید

۴-۲. مشاهده محتوای آرشیو

۴. روی لینک View content کلیک کنید — آرشیو متصل می‌شود
۵. می‌توان چند آرشیو را هم‌زمان باز کرد
۶. هر آرشیو به‌صورت یک root item جدید در User Tree نمایش داده می‌شود

⚠ در حالت مشاهده آرشیو، تمام عملیات تنظیماتی در کنسول غیرفعال می‌شوند. فقط مشاهده داده امکان‌پذیر است.

۴-۳. قطع اتصال آرشیو

- از User Tree: راست‌کلیک روی سرور → Close archive
- از Database management: Archives → Close archive

۴-۴. ستون‌های Records آرشیو

- Date and Time, User Name, Archive Path, Server Name
- Action: Browse database / Connect / Disconnect / Close archive

۵. راهنمای جامع بکاپ‌گیری

۵-۱. آنچه بکاپ داخلی Safetica پوشش می‌دهد

وضعیت	محتوا	دسته
شامل می‌شود	رکوردهای عملیات فایل، لاگ‌های فعالیت کاربران	لاگ‌های فعالیت
شامل می‌شود	رویدادهای شبکه، دستگاه‌ها، چاپ، DLP logs	لاگ‌های رویدادها
شامل نمی‌شود	پالیسی‌های DLP، تنظیمات محصول، ساختار کاربران و گروه‌ها	تنظیمات سیستم
شامل نمی‌شود	Application Integration، Zones Categories	پیکربندی سیستم

⚠ بکاپ داخلی Safetica برای بازیابی کامل سیستم کافی نیست. حتماً بکاپ SQL Server هم انجام دهید.

۵-۲. استراتژی بکاپ کامل — سه لایه ضروری

لایه اول: بکاپ SQL Server (حیاتی‌ترین بخش)

این بکاپ تنها روشی است که می‌تواند کل سیستم Safetica را شامل تمام تنظیمات، پالیسی‌ها و لاگ‌ها در صورت خرابی سرور بازیابی کند.

مراحل انجام بکاپ از طریق SQL Server Management Studio:

۷. SQL Server Management Studio را باز کنید
۸. به سرور SQL متصل شوید
۹. روی دیتابیس safetica_data راست‌کلیک کنید
۱۰. Tasks → Back Up را انتخاب کنید
۱۱. نوع بکاپ را Full انتخاب کنید
۱۲. مسیر ذخیره را روی یک دیسک جداگانه تعیین کنید
۱۳. OK کنید

مسیر پیش‌فرض فایل‌های دیتابیس:

C:\Program Files\Microsoft SQL Server\MSSQL13.SAFETICA\MSSQL\DATA\

فایل‌هایی که باید بکاپ گرفته شوند:

- safetica_data.mdf — فایل اصلی دیتابیس حاوی تمام داده‌ها
- safetica_data_log.ldf — لاگ تراکنش‌های دیتابیس
- safetica_data_FG.ndf — فایل گروه فایلی

لایه دوم: بکاپ داخلی (Safetica Archive)

این بکاپ برای آرشیو کردن تاریخچه لاگ‌ها مناسب است. به‌خصوص برای خارج کردن لاگ‌های قدیمی از دیتابیس عملیاتی در حالی که همچنان قابل‌مشاهده باشند.

۱۴. وارد Tasks → Database management → Maintenance شوید
۱۵. روی New archiving task کلیک کنید
۱۶. نام، نوع Backup، بازه زمانی و مسیر ذخیره را تنظیم کنید
۱۷. Selected objects را مشخص کنید
۱۸. زمان اجرا را برای ساعات کم‌بار (شب) تنظیم کنید

لایه سوم: بکاپ فایل‌های پیکربندی

- مسیر نصب: C:\Program Files\Safetica
- مسیر ProgramData: C:\ProgramData\Safetica
- تنظیمات IIS در صورت استفاده از WebSafetica

۳-۵. مقایسه بکاپ داخلی Safetica با بکاپ SQL

ویژگی	بکاپ داخلی Safetica	بکاپ SQL Server
زمان‌بندی	هر شب نیمه‌شب	تعریف‌شده توسط ادمین
مدت نگهداری	یک ماه	چندین ماه یا بیشتر
محتوا	فقط لاگ‌های فعالیت	تنظیمات + پالیسی‌ها + لاگ‌ها
Restore کامل سیستم	خیر	بله — با SQL Restore
قابل‌مشاهده در کنسول	قابل مشاهده در کنسول	خارج از کنسول Safetica

۴-۵. نکات مهم و هشدارها

بارگذاری سنگین در حین بکاپ

- ارتباط client با دیتابیس ممکن است موقتاً قطع شود
- فرآیند بکاپ ممکن است چند ساعت طول بکشد — بسته به حجم دیتابیس
- در حین بکاپ، Re-indexation انجام ندهید — بکاپ ممکن است fail شود

- بکاپ را حتماً در ساعات کم‌بار (شبانه) برنامه‌ریزی کنید

مدیریت خودکار دیتابیس (Automatic Database Maintenance)

- در تنظیمات پیشرفته می‌توان حداکثر حجم دیتابیس را تعیین کرد:
- در صورت تجاوز از حد تعیین‌شده، قدیمی‌ترین رکوردها به‌طور خودکار حذف می‌شوند
- دیتابیس تا ۷۰٪ حجم تعیین‌شده کاهش می‌یابد
- مثال: تعیین ۱۰۰ گیگابایت → کاهش به حدود ۷۰ گیگابایت

⚠ رکوردهای حذف‌شده در Automatic Maintenance به‌صورت غیرقابل برگشت از بین می‌روند.
قبل از رسیدن به حد مجاز، بکاپ بگیرید.

۵-۵. بازیابی کامل سیستم (Disaster Recovery)

۱۹. Safetica Server را از Universal Installer نصب کنید
۲۰. SQL Server را راه‌اندازی کنید
۲۱. در SQL Management Studio روی Databases راست‌کلیک و Restore Database را انتخاب کنید
۲۲. فایل بکاپ .bak را انتخاب کرده و Restore را اجرا کنید
۲۳. سرویس‌های WebSafetica و Safetica Management Service را راه‌اندازی کنید
۲۴. در صورت نیاز از اسکریپت restart.bat استفاده کنید
۲۵. تنظیمات اتصال سرور به دیتابیس را در Server settings تأیید کنید

۶. محدود کردن آپلود فایل توسط اپلیکیشن خاص

۶-۱. انواع DLP Policy

Safetica از پالیسی‌های DLP برای کنترل عملیات فایل در endpointها استفاده می‌کند. سه نوع وجود دارد:

دسترسی	کاربرد	نوع Policy
همه نسخه‌ها	مدیریت کانال‌های ارتباطی کلی: آپلود، ایمیل، USB و...	General Policy
همه نسخه‌ها	محافظت از داده‌های خاص: شماره کارت، کد ملی، IBAN	Data Policy
فقط Enterprise	کنترل رفتار اپلیکیشن‌ها — برای آپلود یک اپ خاص	Application Policy

⚠ Application Policy فقط در Safetica ONE Enterprise موجود است. در سایر نسخه‌ها از General Policy با تنظیمات Upload استفاده کنید.

۶-۲. روش کار گام‌به‌گام

گام اول: ایجاد Application Category

مسیر: Maintenance → Categories → Applications

- ۲۶. وارد بخش Categories شوید
- ۲۷. اپلیکیشن مورد نظر را در لیست جستجو کنید
- ۲۸. اگر لیست نشده آن را به صورت دستی اضافه کنید
- ۲۹. یک Category جدید فقط برای این اپ تعریف کنید

گام دوم: بررسی Application Integration

مسیر: Maintenance → Integration settings → Application integration

- Active: در تمام کامپیوترها فعال — وضعیت مطلوب
- Inactive: غیرفعال — DLP روی آن اعمال نخواهد شد
- Active (Inactive in test group): همه جا فعال به جز گروه آزمایشی

⚠ اگر اپ در Application Integration فعال نباشد، پالیسی DLP روی آن هیچ تأثیری نخواهد گذاشت.

گام سوم: ایجاد DLP Policy

مسیر: Protection → DLP policies → New policy

۱. نام و توضیح policy را وارد کنید
۲. Policy type را روی Application تنظیم کنید (فقط Enterprise)
۳. Policy mode را انتخاب کنید
۴. در Policy rules، قانون Upload را روی Block تنظیم کنید
۵. Application Category ساخته شده را اضافه کنید
۶. کاربران یا گروه‌های هدف را اضافه کنید
۷. Finish کنید و ذخیره کنید

پس از اعمال policy، حدود ۱۰ دقیقه تا انتقال به Safetica Client منتظر بمانید.

۶-۳. مدهای مختلف Policy

حالت	رفتار سیستم	کاربرد
Disabled	تعریف شده ولی هیچ اثری ندارد	آماده سازی برای اعمال بعدی
Log only	فقط لاگ — هیچ چیزی بلاک نمی شود	تحلیل اولیه جریان داده
Log and notify	هشدار به کاربر + ثبت رویداد — عملیات انجام می شود	آگاه سازی کاربر بدون بلاک
Log and block	بلاک کامل + ثبت رویداد — آپلود غیرممکن	محدودیت کامل — محیط تولیدی

۶-۴. اولویت بندی Policyها

- پالیسی‌ها از بالا به پایین لیست ارزیابی می شوند — اولین تطابق اعمال می شود
- پالیسی‌های خاص تر و سخت گیرانه تر باید در بالای لیست باشند
- برای استثنا یک کاربر: policy جدید بسازید، به همان کاربر بدهید و بالاتر از policy عمومی قرار دهید

۶-۵. مشاهده رویدادها در DLP Logs

مسیر: Protection → DLP logs

- Operation: نوع عملیات — Web upload / Copy / Print / E-mail / IM Send
- Action: نتیجه — Blocked یا Allowed
- Application: اپلیکیشنی که عملیات را انجام داده

- Policy: نام policy اعمال شده

۷. جدول خلاصه — مرجع سریع

موضوع	جزئیات
مسیر بکاپ داخلی	Maintenance → Database management → Tasks
خروجی بکاپ Safetica	دو فایل: mdf (داده) و ldf (لاگ تراکنش)
محتوای بکاپ Safetica	لاگ‌های فعالیت — تنظیمات و پالیسی‌ها شامل نمی‌شود
بکاپ خودکار	هر شب نیمه‌شب — یک ماه نگهداری — جایگزین بکاپ دستی نیست
بکاپ کامل سیستم	SQL Server Full Backup از دیتابیس safetica_data
استراتژی بکاپ کامل	SQL Backup + Archive Safetica + فایل‌های پیکربندی
محدودکردن آپلود یک اپ	Protection → DLP policies → Application Policy (Enterprise فقط)
بررسی یکپارچگی اپ	Maintenance → Integration settings → Application integration

این سند بر اساس [Safetica Complete Documentation EN ۱۰](#) و منابع رسمی support.safetica.com تهیه شده است.