Engineer

Delade upp varje driftshemlighet per värd

Delade upp de fyra driftshemligheterna per värd efter att ha konstaterat att två värdar som delar ett dödmansgrepp larmar mindre än två separata grepp, inte mer, och att en delad lösenfras för säkerhetskopior kan ge tillgång till båda värdarnas kopior, även i separata repon, om någon får tag på den och kan läsa båda reponas krypterade data och nyckelfiler.

september 2026

fyra driftsinställningar med värden som nyckel

Situation. Plattformen byggdes för en värd och skulle snart ha två. Flera operativa hemligheter hade skrivits som enskilda värden utifrån det antagandet: ett repo för säkerhetskopior, en lösenfras, en larmbrytare. Att utvidga dem till en andra värd genom att dela dem är minsta motståndets väg, och det är fel på två separata sätt, som båda misslyckas i tysthet.

Uppgift. Varje hemlighet måste bli en mappning med en nyckel per värd, och skälet måste skrivas ned, eftersom den delade varianten ser korrekt ut och inte kostar något förrän den dag det spelar roll.

Handling. Två argument avgjorde saken, och båda står nedskrivna bredvid konfigurationen. Ett dödmansgrepp som delas av två värdar larmar mindre än två separata grepp, inte mer: så länge någon av värdarna fortfarande pingar förblir kontrollen grön medan den andra är död, och att lägga till en värd i ett delat grepp minskar därför aktivt täckningen för den som redan fanns. Och adressen till ett repo för säkerhetskopior visar var det finns, inte om det har egna åtkomstuppgifter. Separata restic-repon kan ha olika huvudnycklar även om de använder samma lösenfras. Den som får tag på lösenfrasen och kan läsa båda reponas krypterade data och nyckelfiler kan dock låsa upp båda. Delningen innebär alltså en gemensam risk vid en läcka i stället för att isolera värdarna. Varje värde blev en mappning med inventory-värdnamnet som nyckel, uppslagen per värd av en delad task-fil som både konvergenskörningen och förhandskontrollen kör. Den befintliga värden namngavs sedan i alla fyra

mappningarna med sitt repo och båda larmbrytarna lämnade tomma, vilket är det sanningsenliga tillståndet och håller de två öppna initiativen ärliga om att det som återstår är operatörens halva av arbetet och inte koden.

Resultat. Hemligheterna är per värd genom själva konstruktionen, och de två fellägen som skulle ha följt av att dela dem är nedskrivna där nästa person redigerar filen. De tomma posterna är den del som är värd att behålla: de säger att kopplingen finns och att värdet inte gör det, vilket är ett annat och mer användbart besked än en saknad nyckel.

Använd erfarenheten i ert projekt

Använd ”Delade upp varje driftshemlighet per värd” som utgångspunkt för en liknande utmaning i er organisation. Tjänsterna bakom arbetet finns tillgängliga för ert projekt. Hela uppsättningen nedskriven som filer, så att den kan återskapas exakt och aldrig bara finns i en enda persons huvud.

Se våra tjänster Hör av er →

Se bakom resultatet

Läs om situationen, besluten och resultatet i exemplet. Vi kan diskutera vad som passar era förutsättningar och vad som kräver ett annat angreppssätt. Delade upp varje driftshemlighet per värd — fyra driftsinställningar med värden som nyckel

Se våra tjänster Hör av er →

Skulle en enda läckt nyckel exponera alla dina värdar?

Prata om ert projekt med ingenjören som ansvarar för leveransen. Vi avtalar omfattning, hur priset beräknas och överlämning skriftligt innan arbetet börjar.

Roll i uppdraget: Säkerhetsingenjör. Det bygger på Lösningsarkitektur, Infrastruktur, Automatisering och CI/CD, Tillförlitlighet och säkerhetskopiering, Linux och servrar och Säkerhet. Och nu när ni är här: vi är ganska bra på Infrastruktur som kod, Tillförlitlig drift och övervakning, Säkerhetskopiering och återställning, Säkerhet och behörighetshantering och Säkerhet för AI-agenter.

Hör av er Se våra tjänster

En del av **en längre historik** — och den finns i sin helhet här.

Varje post är skriven på samma sätt: situationen, uppgiften, vad vi gjorde och vad som förändrades.

Se hela historiken

Definiera förbättringen ni behöver

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Skulle en enda läckt nyckel exponera alla dina värdar?

Fråga om besluten bakom ”Delade upp varje driftshemlighet per värd”. Ni talar med personer som kan förklara arbetet och bedöma ert eget projekt.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/portfolio/split-every-operational-secret-per-host/