

Obsah

ALM-36 Využitie disku je príliš vysoké	3
ALM-38 Databázový proces je abnormálny.....	7
ALM-44 Využitie databázy je príliš vysoké.....	11
ALM-47 Využitie pamäte služby je príliš vysoké.....	14
ALM-54 Využitie swapu je vysoké	18
ALM-56 Používatelia, ktorí sa príliš dlho neprihlásili	22
ALM-121 Alarm prepnutia na pohotovostný Syslog Server	24
ALM-122 Alarm zlyhania pripojenia hlavného a pohotovostného servera Syslog	26
ALM-128 Pripojenie k hlavnému serveru vzdialenej autentifikácie zlyhalo.....	29
ALM- 151 Využitie CPU je vysoké	32
ALM- 152 Služba OSS je ukončená abnormálne	36
ALM- 154 Využitie pamäte je príliš vysoké	38
ALM-160 Pohotovostné pripojenie k serveru vzdialenej autentifikácie zlyhalo.....	41
ALM-298 Používateľ v skupine SManagers zmení heslo používateľa	44
ALM-299 Používateľ OSS je pridaný do skupiny správcov, SManagers alebo skupiny správcov zabezpečenia subdomén	45
ALM-1067 Záložné dátové balíky neexistujú	46
ALM-30004 Platnosť hesla používateľa čoskoro vyprší	48
ALM-30005 Platnosť hesla používateľa vypršala.....	51
ALM-51020 Platnosť certifikátu čoskoro vyprší	53
ALM-51021 Platnosť certifikátu vypršala	55
ALM-51022 Aktualizácia certifikátu zlyhala	57
ALM-51023 abnormálna služba NTP	58
ALM-51024 Stav stránky je abnormálny.....	66
ALM-51025 Platnosť certifikátu vzdialeného systému DR vypršala	70
ALM-51026 Certifikát vzdialeného systému DR čoskoro skončí	71
ALM-51027 Preťaženie dokumentov	72
ALM-100003 Platnosť certifikátu čoskoro vyprší.....	75
ALM-100005 Platnosť certifikátu vypršala	81
ALM-100006 Zlyhania autentifikácie dosahujú maximum.....	86
ALM-100007 Abnormálna kontrola stavu poplachovej služby.....	88
ALM-100450 Zistila sa nezákonná požiadavka	90
ALM-100503 Test pripojenia oblasti nasadenia zlyhal.....	93
ALM-101200 Abnormálna replikácia	94

ALM-101201 Abnormálny srdcový tep.....	101
ALM-101205 Zlyhanie plánovaného zálohovania údajov o produkte.....	107
ALM-101206 Kanál správy SSH je chybný.....	112
ALM-101207 Zlyhanie príjmu alarmov v dôsledku odpojenia zariadenia.....	116
ALM-101208 Stav uzla je Abnormálny.....	119
ALM-101210 Stav lokálnej kópie databázy je abnormálny.....	123
ALM-101216 Plánované zlyhanie zálohovania.....	126
ALM-101217 Zlyhanie plánovaného zálohovania aplikácie produktu.....	131
ALM-101218 Zlyhanie plánovaného zálohovania databázovej aplikácie.....	136
ALM-101219 Plánované zlyhanie zálohovania operačného systému.....	141

ALM-36 Využitie disku je príliš vysoké

Popis alarmu

Tento alarm sa generuje, keď PowerEcho zistí (detekcia sa vykonáva každých 60 sekúnd) , že využitie disku alebo oddielu je väčšie alebo rovné prahu generovania alarmu pre N (N sú časy preťaženia) po sebe idúcich časov. Tento alarm sa automaticky vymaže, keď je využitie disku alebo diskového oddielu nižšie ako prah pre vymazanie alarmu.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
36	Major	Cez limit

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Operačný systém	OS servera.
	Disk	Názov disku servera, pre ktorý sa generuje alarm.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	Generačný prah	Prahová hodnota pre vygenerovanie alarmu.
	Prahová hodnota	Prahová hodnota pre zrušenie alarmu.
	Kapacita	Kapacita disku.
	Použitie	Využitie miesta na disku.
	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

Operácia zápisu služby PowerEcho môže zlyhať a môže sa vyskytnúť výnimka databázy.

Možné príčiny

- Prah generovania alarmu pre využitie diskového priestoru uzla je nevhodný.
- Disk obsahuje príliš veľa nepotrebných súborov.
 - Kôš nie je vyčistený.
 - Server prijal veľké množstvo údajov vrátane alarmov NE, udalostí a protokolov. Dáta sa v krátkom čase exportujú z databázy na diskové súbory.
 - Existuje príliš veľa dočasných dátových súborov a záložných súborov.

Postup

1. Prihláste sa do PowerEcho.
 - a. Prístup k PowerEcho získate na `https://client IP address PowerEcho:31945`.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Skontrolujte, či sú prahové hodnoty pre tento alarm vhodné.
 - a. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Threshold Rule Settings**.
 - b. Na navigačnej table vyberte položku **Exception and Event Thresholds**.
 - c. V ľavom hornom rohu stránky **Exception and Event Thresholds** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias** a skontrolujte, či sú prahové hodnoty pre tento alarm vhodné.
 - Ak áno, prejdite na 3.
 - Ak nie, nastavte príslušné prahové hodnoty a prejdite na 4.
 3. Odstráňte nepotrebné súbory z diskov.
 - a. Použite PuTTY na prihlásenie sa do chybného uzla ako používateľ **sopuser** v režime SSH.
 - b. Ak chcete prepnúť na používateľa **root**, spustite nasledujúci príkaz:
su - root
`Password: password for the root user`
 - c. Spustite nasledujúci príkaz na identifikáciu disku s vysokým využitím miesta:
df -k

NOTE

Ak disky, ktoré nie sú uvedené v parametri **Disk** alarm, majú vysoké využitie disku, ale využitie je nižšie ako prah pre generovanie alarmu, môžete tiež vymazať nepotrebné súbory z diskov.

- d. Spustíte nasledujúce príkazy, aby ste prešli do adresára disku s vysokým zaťažením, spýtali sa súborov a podadresárov na disku, zoradili súbory a podadresáre podľa veľkosti a zapísali súbory a podadresáre do súboru **du_k.txt**.

cesta k súboru **cd**

ty -k | sort -nr > /tmp /du_k.txt

- e. Spustíte nasledujúci príkaz, aby ste skontrolovali súbor **du_k.txt** a identifikovali podadresár väčšej veľkosti:

viac /tmp /du_k.txt

- f. Spustením nasledujúcich príkazov prejdite do podadresára väčšej veľkosti, dotazujte sa na súbory a podadresáre v podadresári, zoradte súbory a podadresáre podľa veľkosti a zapíšte súbory a podadresáre do súboru **ls_l.txt**.

cesta k súboru **cd**

ls -l | sort -nr > /tmp /ls_l.txt

- g. Spustíte nasledujúci príkaz, aby ste skontrolovali súbor **ls_l.txt** a identifikovali podadresár alebo súbor väčšej veľkosti:

viac /tmp /ls_l.txt

- h. Spustíte nasledujúci príkaz na ukončenie od používateľa **root**:

exit

- i. Opakujte kroky 3.d až 3.h, aby ste našli súbory, ktoré spôsobujú vysoké využitie disku, a zistíte, ktoré z nich sú nepotrebné súbory, a potom tieto súbory vymažte. Odporúčame vám vymazať predtým zálohované inštalačné balíky, záplatové balíky, inštalačné balíky adaptačnej vrstvy, záložné súbory počas inštalácie a základné súbory. Nepotrebné súbory PowerEcho a databázy je možné odstrániť. Po odstránení súborov prejdite na 4.

NOTE

Ak si nie ste istí, či je možné súbor odstrániť, kontaktujte technickú podporu.

4. Počkajte 1 minútu a potom skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, zozbierajte predchádzajúce informácie o spracovaní alarmu a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm na PowerEcho, vyberte **Maintenance > Operation and Maintenance Management > Exceptions and Events** a kliknite na **Clear** vstúpci **Operation** pri alarme na karte **Exceptions**.

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Verzia operačného systému uzla, pre ktorý sa generuje tento alarm, sa zmenila.
- Bod pripojenia disku, pre ktorý sa generuje tento alarm, sa zmenil.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM-38 Databázový proces je abnormálny

Popis alarmu

Tento alarm sa generuje, keď sa proces databázy neočakávane zastaví na 4 minúty. Ak sa proces databázy po nahlásení alarmu obnoví, tento alarm sa automaticky vymaže.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
38	Major	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Operačný systém	Operačný systém servera.
	Databázová služba	Názov inštancie databázy, pre ktorú sa generuje alarm.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

Služby nemajú prístup k databáze. Ak porucha trvá dlhší čas, informácie o alarme sa stratia alebo SmartPVMS nebude k dispozícii.

Možné príčiny

Po výnimke sa nepodarí reštartovať databázový proces.


Postup

1. Spustíte abnormálnu databázovú službu. Skontrolujte, či hodnota parametra alarmu **Product alias** patrí do PowerEcho. Odstráňte poruchu podľa tabuľky 1.

Tabuľka 1 Návod na obsluhu

Skontrolujte výsledok	Spôsob prevádzky
<p>Hodnota parametra alarmu Product alias patrí do PowerEcho.</p>	<p>Spustite abnormálnu databázovú službu PowerEcho .</p> <ol style="list-style-type: none"><li data-bbox="863 387 1469 495">1. Použite PuTTY na prihlásenie do riadiaceho uzla ako používateľ sopuser v režime SSH.<li data-bbox="863 524 1469 674">2. Ak chcete prepnúť na používateľa ossadm , spustíte nasledujúci príkaz : su – ossadm Heslo: <i>heslo pre používateľa ossadm</i> <pre data-bbox="908 696 1495 723">Password: password for the ossadm user</pre> <ol style="list-style-type: none"><li data-bbox="863 730 1469 954">3. Spustíte nasledujúce príkazy na spustenie abnormálnej databázovej služby: source installation directory /manager /bin/engr_profile.sh ipmc_adm -cmd startdc -tenant manager -instance database service <p>POZNÁMKA: <i>databázová služba odkazuje na Database service v časti Location Info.</i> Ak sa zobrazia informácie podobné nasledujúcim, databázová služba sa úspešne spustí. V opačnom prípade kontaktujte technickú podporu.</p> <pre data-bbox="908 1263 1495 1368">... ===== Starting data container processes is complete.</pre>
<p>Hodnota parametra alarmu Product alias nepatrí do PowerEcho.</p>	<p>Spustíte abnormálnu databázovú službu produktu.</p> <ol style="list-style-type: none"><li data-bbox="863 1458 1469 1525">4. Prístup k PowerEcho získate na https://client IP address of the PowerEcho:31945. <p>POZNÁMKA: Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.</p> <ol style="list-style-type: none"><li data-bbox="863 1794 1469 1906">5. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo Log In.

Tabuľka 1 Návod na obsluhu

Skontrolujte výsledok	Spôsob prevádzky
	<ol style="list-style-type: none">6. Z hlavnej ponuky vyberte Maintenance > Operation and Maintenance Management > Panoramic Monitoring.7. Na navigačnej table vyberte položku Middleware Monitoring.8. V ľavom hornom rohu stránky Middleware Monitoring vyberte produkt zodpovedajúci hodnote parametra alarmu Product alias.9. V pravom hornom rohu stránky skontrolujte, či niektorý zdroj v Relational Databases a Redis Databases nie je abnormálny. <p>POZNÁMKA: Číslo v červenej farbe označuje počet abnormálnych zdrojov.</p> <ul style="list-style-type: none">• Ak áno, na navigačnej table vyberte položku Node Monitoring. V ľavom hornom rohu stránky Node Monitoring vyberte v detailoch alarmu produkt zodpovedajúci Product aliasu. Kliknite  na stĺpec Operation v riadku, ktorý obsahuje uzol, ku ktorému patrí abnormálna inštancia databázy.• Ak nie, chyba nie je spôsobená abnormálnymi databázami, kontaktujte technickú podporu.

2. Po spustení databázovej služby počkajte 5 minút a skontrolujte, či je alarm vymazaný.

- Ak áno, nie sú potrebné žiadne ďalšie kroky.
- Ak nie, kontaktujte technickú podporu .

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm n aPowerEcho, vyberte **Maintenance >**

Operation and Maintenance Management > Exceptions and Events a kliknite na **Clear** v stĺpci **Operation** pri alarme na karte **Exceptions**.

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM-44 Využitie databázy je príliš vysoké

Popis alarmu

Tento alarm sa generuje, keď PowerEcho zistí (detekcia sa vykonáva každých 60 sekúnd), že využitie tabuľkového priestoru databázy alebo využitie pamäte databázy Redis je väčšie alebo rovné prahu generovania alarmu pre N (N sú časy preťaženia) po sebe idúcich časov. Tento alarm sa automaticky vymaže, keď je využitie databázového tabuľkového priestoru alebo využitie pamäte databázy Redis nižšie ako prah zrušenia alarmu.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
44	Major	Cez limit

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Databázová služba	Názov inštancie databázy, pre ktorú sa generuje alarm.
	Databáza	Názov databázy, pre ktorú sa generuje alarm.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	Veľkosť	Veľkosť veľkosti databázového tabuľkového priestoru alebo pamäte databázy Redis.
	Prah	Prahová hodnota pre vygenerovanie alebo zrušenie alarmu.
	Použitie	Použitie tabuľkového priestoru relačnej databázy alebo pamäte databázy Redis.
	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

Ak je využitie databázového tabuľkového priestoru alebo pamäte databázy Redis príliš vysoké, operácie súvisiace s databázou môžu zlyhať. V dôsledku toho môžu byť príslušné servisné funkcie databázy nedostupné.

Možné príčiny

- Prah generovania alarmu pre databázový tabuľkový priestor alebo pamäť databázy Redis uzla je nevhodný.
- Databázový tabuľkový priestor alebo databázová pamäť Redis nie je uvoľnená včas po exportovaní alebo výpise údajov v databáze.

Postup

1. Prihláste sa do PowerEcho .
 - a. Prístup k PowerEcho získate na **https:// *klientská IP adrese* PowerEcho:31945** .

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In** .
2. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Threshold Rule Settings** .
 3. Na navigačnej table vyberte položku **Exception and Event Thresholds**.
 4. V ľavom hornom rohu stránky **Exception and Event Thresholds** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias**.
 5. Skontrolujte, či sú hodnoty prahov pre **The Database Usage Is Too High**.
 - Ak áno, kontaktujte technickú podporu.
 - Ak nie, nastavte príslušné prahové hodnoty a prejdite na 6.
 6. Počkajte 1 minútu a potom skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, zozbierajte predchádzajúce informácie o spracovaní alarmu a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm na PowerEcho, vyberte **Maintenance > Operation and Maintenance Management > Exceptions and Events** a kliknite na **Clear** v stĺpci **Operation** alarmu nakarte **Exceptions**.

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM-47 Využitie pamäte služby je príliš vysoké

Popis alarmu

Systém kontroluje využitie pamäte službou každých 60 sekúnd. Tento alarm sa generuje, keď je využitie pamäte službou väčšie alebo rovné prednastavenej prahovej hodnote pre N po sebe idúcich časov (N je nastavené v konfiguračnom súbore a môže byť číslo od 1 do 999). Tento alarm sa automaticky vymaže, keď je využitie pamäte službou menšie ako prednastavený prah.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
47	Major	Cez limit

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Operačný systém	OS servera.
	servis	Názov mikroslužby, pre ktorú sa generuje alarm.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	Prah	Prah generovania alarmu a prah zrušenia alarmu.
	Použitie	Pamäť používaná službami.
	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

Server SmartPVMS reaguje pomaly.

Možné príčiny

Vyskytla sa chyba programu.

Postup

1. Skontrolujte , či hodnota **Host** v parametroch alarmu patrí do PowerEcho.
 - Ak áno, prejdite na 2.
 - Ak nie, prejdite na 3.
2. Reštartujte službu PowerEcho.
 - a. Použite PuTTY na prihlásenie do riadiaceho uzla ako používateľ **sopuser** v režime SSH.
 - b. Ak chcete prepnúť na používateľa **ossadm** , spustite nasledujúci príkaz:

su - ossadm

```
Password: password for the ossadm user
```

- c. Spustite nasledujúce príkazy na spustenie procesu HyperHA:

NOTE

Ak je PowerEcho nasadené v režime klastra , vykonajte operáciu na Management0 a Management1 v poradí.

```
source installation directory/manager/bin/engr_profile.sh
```

```
ipmc_admin -cmd startapp -app HyperHAService -tenant manager
```

Ak sa zobrazia nasledujúce informácie a zobrazí sa **success** procesu, spustí sa HyperHA. V opačnom prípade kontaktujte technickú podporu.

```
Starting process hyperhaagent-1-0 ... success
```

- d. Spustite nasledujúce príkazy na reštartovanie služby PowerEcho:

```
source installation directory/manager/bin/engr_profile.sh
```

```
ipmc_admin -cmd restartapp -tenant manager
```

NOTE

Ak je PowerEcho nasadené v režime klastra , spustite službu na Management0 , Management1 a potom Management2 . To znamená, že službu spustite na Management1 ihneď po spustení príkazu na spustenie na Management0 a spustite službu na Management2 ihneď po spustení príkazu na spustenie na Management1 . Po spustení služieb na všetkých uzloch skontrolujte výsledok spustenia každého uzla. Ak spustenie na uzle zlyhá, kontaktujte technickú podporu .

Ak sa zobrazia informácie podobné nasledujúcim a zobrazí sa **success** pre všetky procesy, všetky služby v uzle sa úspešne reštartujú. V opačnom prípade kontaktujte technickú podporu.

```
...  
Stopping process deployapp-0-0 ... success  
Stopping process mczkapp-0-0 ... success  
Stopping process etcd-0-0 ...success
```

```
...
Starting process deployapp-0-0 ... success
Starting process mczkapp-0-0 ...success
Starting process etcd-0-0 ... success
...
```

- e. Skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

3. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
- c. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Panoramic Monitoring**.
- d. Na navigačnej table vyberte položku **Node Monitoring**.
- e. V ľavom hornom rohu stránky **Node Monitoring** vyberte produkt zodpovedajúci hodnote parametra alarmu **Prodct alias**.
- f. V oblasti **Node List** kliknite na názov uzla, pre ktorý sa generuje alarm.
- g. Na navigačnej table vyberte položku **Service Monitoring**.
- h. Na karte **Processes** vyberte proces, pre ktorý sa generuje alarm, a kliknite na tlačidlo **Stop**. Keď sa stav procesu zmení na **Not Running**, kliknite na tlačidlo **Start**.

NOTE

Názov procesu, pre ktorý sa generuje alarm, môžete získať v časti **Location Info** o mieste alarmu.

4. Po spustení procesu počkajte 5 minút a skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm na PowerEcho, vyberte **Maintenance > Operation and Maintenance Management > Exceptions and Events** a kliknite na **Clear** v stĺpci **Operation** alarmu na karte **Exception**

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM-54 Využitie swapu je vysoké

Popis alarmu

Tento alarm sa generuje, keď PowerEcho zistí (detekcia sa vykonáva každých 60 sekúnd) , že využitie virtuálnej pamäte je väčšie alebo rovné prahu generovania alarmu pre N (N sú časy preťaženia) po sebe idúcich časov. Tento alarm sa automaticky vymaže, keď je využitie virtuálnej pamäte menšie ako prah zrušenia alarmu.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
54	Kritické	Cez limit

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Operačný systém	OS servera.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	Generačný prah	Prahová hodnota pre vygenerovanie alarmu.
	Prahová hodnota	Prahová hodnota pre zrušenie alarmu.
	Využitie virtuálnej pamäte	Využitie virtuálnej pamäte.
	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

- Dostupná pamäť PowerEcho sa znižuje, odozva je pomalá a operácie sa oneskorujú.
- Proces sa môže stať abnormálnym, čo môže spomaliť spracovanie služby a môžu sa hromadiť správy a systém sa môže zrušiť.
- Odkladací priestor sa často používa, čo zhoršuje výkon PowerEcho a oneskoruje zber informácií. Výsledkom je oneskorenie výkonu v reálnom čase a hlásenie alarmových údajov.

Možné príčiny

- Prah generovania alarmu pre využitie virtuálnej pamäte uzla je nevhodný.
- Vykonávajú sa operácie náročné na systémové prostriedky.

Postup

1. Prihláste sa do PowerEcho.
 - a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Threshold Rule Settings**.
 3. Na navigačnej table vyberte položku **Exception and Event Thresholds**.
 4. V ľavom hornom rohu stránky **Exception and Event Thresholds** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias** a skontrolujte, či sú prahové hodnoty pre tento alarm vhodné.
 - Ak áno, prejdite na 5.
 - Ak nie, nastavte príslušné prahové hodnoty a prejdite na 8.
 5. Skontrolujte procesy s veľkou veľkosťou použitej virtuálnej pamäte v uzle, kde sa generuje alarm.
 - a. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Panoramic Monitoring**.
 - b. Na navigačnej table vyberte položku **Node Monitoring**.
 - c. V ľavom hornom rohu stránky **Node Monitoring** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias**.
 - d. V zozname uzlov kliknite na názov uzla zodpovedajúci hodnote **Host** v parametroch alarmu.
 - e. Na karte **Processes** na stránke **Node Details** zoradíte stĺpec **Virtual Memory** v zostupnom poradí a skontrolujte, či existujú procesy s veľkou veľkosťou použitej virtuálnej pamäte.
 - Ak áno, zozbierajte predchádzajúce informácie o spracovaní alarmov a kontaktujte technickú podporu. Skontrolujte, či je alarm vymazaný. Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. Ak alarm pretrváva, prejdite na 6.

- Ak nie, prejdite na 6.

6. Skontrolujte procesy s veľkou veľkosťou použitej virtuálnej pamäte (okrem tých v 5) v uzle, kde sa generuje alarm.

- Použite PuTTY na prihlásenie do chybného uzla uvedeného v detailoch alarmu ako používateľ **sopuser** v režime SSH.
- Spustíte nasledujúci príkaz a skontrolujte, či existujú procesy, ktorých využitie virtuálnej pamäte je vyššie ako pri iných procesoch:

top -o VIRT

Zobrazia sa informácie podobné nasledujúcim. Hodnoty v stĺpci **VIRT** sú zobrazené v zostupnom poradí. Stlačte **Ctrl + C**.

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4098516	ossadm	20	0	7263988	392028	19124	S	0.3	1.2	1:28.91	java
3962012	ossadm	20	0	6370712	25500	9608	S	0.7	0.1	1:47.16	nodeagent
4052885	ossadm	20	0	2284080	602544	21240	S	0.3	1.9	5:33.63	java
3954155	ossadm	20	0	2226912	65208	20204	S	1.0	0.2	2:58.55	odbp
2754	polkitd	20	0	1926924	14808	7816	S	0.0	0.0	147:49.42	polkitd
...											

- Ak áno, zozbierajte predchádzajúce informácie o spracovaní alarmov a kontaktujte technickú podporu.
Skontrolujte, či je alarm vymazaný. Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. Ak alarm pretrváva, prejdite na 7.
- Ak nie, prejdite na 7.

7. Skontrolujte, či sa využitie virtuálnej pamäte uzla stále zvyšuje.

- Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Panoramic Monitoring**.
- Na navigačnej table vyberte položku **Node Monitoring**.
- V ľavom hornom rohu stránky **Node Monitoring** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias**.
- V zozname uzlov nájdite názov uzla zodpovedajúci **Host** v parametroch alarmu.
- Skontrolujte, či sa využitie virtuálnej pamäte uzla stále zvyšuje.

- Ak áno, zozbierajte predchádzajúce informácie o spracovaní alarmov a kontaktujte technickú podporu. Nevyžadujú sa žiadne ďalšie kroky.
- Ak nie, prekonfigurujte prahové hodnoty pre tento alarm na stránke **Threshold Rule Settings** a prejdite na 8.

8. Počkajte 1 minútu a potom skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, zozbierajte predchádzajúce informácie o spracovaní alarmu a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm na PowerEcho, vyberte **Maintenance > Operation and Maintenance Management > Exceptions and Events** a kliknite na **Clear** v stĺpci **Operation** alarmu nakarte **Exceptions**.

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Verzia operačného systému uzla, pre ktorý sa generuje tento alarm, sa zmenila.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM-56 Používatelia, ktorí sa príliš dlho neprihlásili

Popis alarmu

Tento alarm sa generuje, keď používateľ po sebe nasleduje čas offline (štandardne 60 dní) na SmartPVMS dosiahne čas uvedený v politike pre vymazanie alebo zakázanie užívateľa.

NOTE

Používateľská politika pre neprihlásenie v rámci určitého obdobia je nakonfigurovaná takto:

- **Ak je nakonfigurovaná osobná politika:** Vyberte **System > System Management > User Management** z hlavnej ponuky. V zozname **Users** upravte v časti **Basic Information** možnosť **Enable the user policy if no login within a period**.
- **Ak osobná politika nie je nakonfigurovaná:** Z hlavnej ponuky vyberte **System > System Management > User Policies**. V **Account Policy** zmeňte možnosť **Enable account suspension** a **Enable the user policy if no login within a period**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
56	Major	Bezpečnostný alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Používateľské meno	Meno používateľa, ktorý bol odstránený alebo zakázaný z dôvodu žiadneho SmartPVMS prihlásenie na zadané po sebe nasledujúce dni.
	Manipulačná politika	Režim spracovania pre používateľa, ktorý sa neprihlási počas zadaných po sebe nasledujúcich dní.
	Dátum	Dátum odstránenia alebo deaktivácie používateľského účtu.
Ďalšie informácie	Dni neprihlásenia	Počet po sebe nasledujúcich dní bez prihlásenia uvedený v zásade.

Vplyv na systém

Vymazaní alebo zakázaní používatelia nemajú prístup do systému.

Možné príčiny

Používateľ je odstránený alebo zakázaný, pretože nie je SmartPVMS prihlásenie na dlhú dobu.

Postup

Skontrolujte, či chcete pokračovať v používaní používateľského účtu. Ak áno, kontaktujte bezpečnostných správcov.

Vymazanie alarmu

ADMC: Po odstránení poruchy musíte tento alarm manuálne vymazať.

ALM-121 Alarm prepnutia na pohotovostný Syslog Server

Popis alarmu

Tento alarm sa generuje, ak sa systém prepne na pohotovostný server Syslog, pretože aktívny server sa nedá pripojiť. Vymaže sa po úspešnom pripojení systému a prepnutí späť na aktívny server Syslog.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
121	Major	Environmentálny alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	IP hlavného servera	IP adresa aktívneho servera Syslog.
	Port hlavného servera	Číslo portu aktívneho servera Syslog.
	IP servera v pohotovostnom režime	IP adresa pohotovostného servera Syslog.
	Port servera v pohotovostnom režime	Číslo portu servera Syslog v pohotovostnom režime.

Vplyv na systém

Protokoly sa posielajú na pohotovostný server Syslog namiesto aktívneho servera Syslog.

Systémové akcie

Ak nie je možné pripojiť aktívny Syslog server, systém sa prepne na pohotovostný Syslog server.

Možné príčiny

- Aktívny server Syslog nie je spustený.
- Systém je odpojený od aktívneho servera Syslog.

Postup

1. Skontrolujte, či je spustený aktívny server Syslog.
 - Ak nie, spustíte aktívny server Syslog a prejdite na 3.
 - Ak áno, prejdite na 2.

NOTE

Servery Syslog sú servery tretích strán. Podrobnosti o tom, ako skontrolovať ich stav, nájdete v súvisiacom popise servera.

2. Skontrolujte, či je systém správne pripojený k aktívnemu serveru Syslog.
 - a. Získajte IP adresu aktívneho servera Syslog (**Master server IP**) z **Location Info** o polohe alarmu.
 - b. Použite PuTTY na prihlásenie do uzla, kde sídli SMLogLic, ako používateľ **sopuser** v režime SSH. Podrobnosti o tom, ako získať adresu IP uzla, v ktorom sa nachádza služba, nájdete v časti "Querying the Management IP Address of the Node Where a Process or Service Resides" in *Administrator Guide*.
 - c. Ak chcete prepnúť na používateľa **ossadm**, spustíte nasledujúci príkaz:
su - ossadm

```
Password: heslo pre používateľa ossadm
```

- d. Skontrolujte sieťové pripojenie medzi systémom a aktívnym serverom Syslog.
 - Pre adresu IPv4 spustíte nasledujúci príkaz:
ping *IP address of the active Syslog server*
 - Pre adresu IPv6 spustíte nasledujúci príkaz:
Ping6 *IP address of the active Syslog server*

Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Stlačením **Ctrl+C** zastavíte príkaz ping.

```
64 bytes from IP address of the active Syslog server: icmp_seq=1 ttl=62  
time=2.20 ms
```

Ak sa do 1 minúty nevrátia žiadne informácie, sieťové pripojenie je abnormálne. Stlačením **Ctrl+C** zastavíte príkaz ping a opravíte chybu siete.

3. Počkajte 30 sekúnd a skontrolujte, či je alarm vymazaný.
 - Ak áno, nie sú potrebné žiadne ďalšie kroky.
 - Ak nie, získajte informácie o spracovaní alarmov a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-122 Alarm zlyhania pripojenia hlavného a pohotovostného servera Syslog

Popis alarmu

Tento alarm sa generuje, ak sa systému nepodarí pripojiť k aktívnym a pohotovostným serverom syslog. Vymaže sa po úspešnom pripojení systému k aktívnemu alebo pohotovostnému serveru syslog.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
122	Major	Environmentálny alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	IP hlavného servera	IP adresa aktívneho servera syslog.
	Port hlavného servera	Číslo portu aktívneho servera syslog.
	IP servera v pohotovostnom režime	IP adresa pohotovostného servera syslog.
	Port servera v pohotovostnom režime	Číslo portu servera syslog v pohotovostnom režime.

Vplyv na systém

Ak sa vyskytne tento alarm, protokoly nie je možné preposlať na aktívny alebo pohotovostný server syslog. Tento alarm bude vymazaný, keď sa systém úspešne pripojí k aktívnemu alebo pohotovostnému syslog serveru. Po odstránení alarmu budú protokoly, ktoré spĺňajú podmienky preposielania, odoslané na aktívny alebo pohotovostný server syslog.

Systémové akcie

žiadne

Možné príčiny

- Parametre servera syslog sú nesprávne.
- Aktívny a pohotovostný server syslog nie sú spustené.
- Systém je odpojený od aktívnych a pohotovostných serverov syslog.

Postup

1. Skontrolujte nastavenia parametrov servera syslog.
 - a. Z hlavnej ponuky vyberte **System > Log Management > Log Dump**.
 - b. Na navigačnej table vyberte **Forwarding Server**.
 - c. Na stránke **Forwarding Server** skontrolujte, či sú parametre servera syslog správne.
 - I. Ak áno, prejdite na 2.
 - II. Ak nie, upravte parametre servera syslog a prejdite na 4.
2. Skontrolujte, či sú spustené aktívne a pohotovostné servery syslog.
 - Ak áno, prejdite na 3.
 - Ak nie, spustíte aktívny a pohotovostný syslog server a prejdite na 4.

NOTE

Servery Syslog sú servery tretích strán. Podrobnosti o tom, ako skontrolovať ich stav, nájdete v súvisiacom popise servera.

3. Skontrolujte, či je systém správne pripojený k aktívnym a pohotovostným serverom syslog.
 - a. Získajte IP adresy aktívnych a pohotovostných serverov syslog (**Master server IP a Standby server IP**) z **Location Info** o polohe alarmu.
 - b. Použijete PuTTY na prihlásenie do uzla, kde sídli SMLogLic, ako používateľ **sopuser** v režime SSH. Podrobnosti o tom, ako získať adresu IP uzla, v ktorom sa nachádza služba, nájdete v časti „Querying the Management IP Address of the Node Where a Process or Service Resides“ in *Administrator Guide*.
 - c. Ak chcete prepnúť na používateľa **ossadm**, spustíte nasledujúci príkaz :
su - ossadm
 - d. Skontrolujte sieťové pripojenie medzi systémom a aktívnym a pohotovostným syslog serverom.
 - Pre adresu IPv4 spustíte nasledujúci príkaz:
ping IP address of the syslog server
 - Pre adresu IPv6 spustíte nasledujúci príkaz:
Ping6 IP address of the syslog server

Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Stlačením **Ctrl + C** zastavte príkaz ping a prejdite na 4 .

```
64 bytes from IP address: icmp_seq=1 ttl=62 time=2.20 ms
```

Ak sa do 1 minúty nevrátia žiadne informácie, sieťové pripojenie je abnormálne. Stlačením **Ctrl+C** zastavíte príkaz ping a opravíte chybu siete.

4. Počkajte 30 sekúnd a skontrolujte, či je alarm vymazaný.

- Ak áno, nie sú potrebné žiadne ďalšie kroky.
- Ak nie, získajte informácie o spracovaní alarmov a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-128 Pripojenie k hlavnému serveru vzdialenej autentifikácie zlyhalo

Popis alarmu

Ak je povolená autentifikácia LDAP a **User authentication mode** je nastavený na možnosť **Fixed user**, SmartPVMS alebo PowerEcho kontroluje pripojenia s aktívnymi a pohotovostnými servermi LDAP v určenom intervale. Interval kontroly je štandardne päť minút. Tento alarm sa generuje, keď je SmartPVMS alebo PowerEcho, že pripojenie k aktívnemu serveru LDAP je abnormálne. Tento alarm sa automaticky vymaže, keď sa pripojenie k aktívnemu serveru LDAP stane normálnym.

NOTE

Interval kontroly je možné nastaviť v časti **Server check interval** v **LDAP Authentication**.

1. Vykonajte operácie na základe zdroja alarmu.
 - TheSmartPVMS : Prihláste sadoSmartPVMS .Z hlavnej ponuky vyberte **System > System Management > Authentication**.
 - PowerEcho : Prihláste sa do PowerEcho . Z hlavnej ponuky vyberte **System > Security Management > Authentication**.
2. Na navigačnom paneli vyberte položku **Remote Authentication**.
3. Na stránke **Remote Authentication** kliknite na **LDAP Authentication**. Nastavte **Server check interval**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
128	Kritické	Environmentálny alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	IP servera	Adresa aktívneho servera LDAP.
Ďalšie informácie	Typ služby	Režim vzdialenej autentifikácie.
	typ produktu	Ak je zdrojom alarmu PowerEcho , tento parameter je uvedený v detailoch alarmu.

Vplyv na systém

Pri autentifikácii LDAP nemôže aktívny server LDAP poskytovať službu autentifikácie.

Možné príčiny

- Aktívny server LDAP nie je spustený.

- TheSmartPVMS je odpojený od aktívneho servera LDAP.
- PowerEcho je odpojený od aktívneho servera LDAP.

Postup

1. Skontrolujte hodnotu **Server IP** v **Location Info** alarmu, ktorá označuje adresu aktívneho servera LDAP.
2. Skontrolujte, či aktívny server LDAP funguje správne.

NOTE

Server LDAP poskytujú zákazníci na vzdialenú autentifikáciu. Kontaktujte správcu zákazníka, aby skontroloval, či server funguje správne.

- Ak aktívny server LDAP nebeží, spustíte aktívny server LDAP a prejdite na 5.
 - Ak aktívny server LDAP funguje správne, prejdite na 3.
3. Skontrolujte, či SmartPVMS je správne pripojený k aktívnemu serveru LDAP.
 - a. Použijete PuTTY na prihlásenie do uzla, kde sídli SMLogLic alebo používateľský proces SM, ako používateľ **sopuser** v režime SSH. Podrobnosti o tom, ako získať adresu IP uzla, v ktorom sa nachádza proces alebo služba, nájdete v časti „Dopyt na adresu IP správy uzla, v ktorom sa nachádza proces alebo služba“ v *príručke správcu*.
 - b. Skontrolujte, či je systém správne pripojený k aktívnemu serveru LDAP.
 - Ak je adresa IP adresou IPv4, spustíte nasledujúci príkaz:
ping *IP address of the active LDAP server*
 - Ak je adresa IP adresou IPv6, spustíte nasledujúci príkaz:
ping6 *IP address of the active LDAP server*

Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Stlačením **Ctrl+C** príkaz zastavíte.

```
64 bytes from address of the active LDAP server
```

Ak sa do 1 minúty nevrátia žiadne informácie, sieťové pripojenie je abnormálne. Stlačením klávesov **Ctrl+C** zastavte príkaz a opravte poruchu siete.
 4. Skontrolujte, či je PowerEcho správne pripojené k aktívnemu serveru LDAP.
 - a. Použijete PuTTY na prihlásenie do riadiaceho uzla ako používateľ **sopuser** v režime SSH.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 alebo Management1. Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Querying the Management IP Address of the Node Where a Process or Service Resides“ in *Administrator Guide*.

b. Skontrolujte, či je systém správne pripojený k aktívnemu serveru LDAP.

- Ak je adresa IP adresou IPv4, spustíte nasledujúci príkaz:
ping *IP address of the active LDAP server*
- Ak je adresa IP adresou IPv6, spustíte nasledujúci príkaz:
ping6 *IP address of the active LDAP server*

Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Stlačením **Ctrl+C** príkaz zastavíte.

```
64 bytes from address of the active LDAP server
```

Ak sa do 1 minúty nevrátia žiadne informácie, sieťové pripojenie je abnormálne. Stlačením klávesov **Ctrl+C** zastavte príkaz a opravte poruchu siete.

5. Počkajte 5 minút a skontrolujte, či je alarm vymazaný.

NOTE

Interval, v ktorom sa alarm vymaže, je rovnaký ako hodnota **Server check interval**. Predvolená hodnota je 5 minút.

- Ak áno, nie sú potrebné žiadne ďalšie kroky.
- Ak nie, získajte informácie o spracovaní alarmov a kontaktujte technickú podporu .

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM- 151 Využitie CPU je vysoké

Popis alarmu

PowerEcho postupne vzorkuje využitie CPU servera. Tento alarm sa generuje, keď každé vzorkované využitie CPU v perióde vzorkovania (počet preťažení x 60 sekúnd) je väčšie alebo rovné prahu generovania alarmu. Tento alarm sa automaticky vymaže, keď je jedno vzorkovanie CPU v perióde vzorkovania menšie ako prah zrušenia alarmu.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
151	Major	Cez limit

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Operačný systém	OS servera.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	Generačný prah	Prahová hodnota pre vygenerovanie alarmu.
	Prahová hodnota	Prahová hodnota pre zrušenie alarmu.
	vyuzitie procesora	využitie CPU servera.
	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.


Vplyv na systém

- Uzol, pre ktorý sa generuje alarm, reaguje pomaly a operácie súvisiace s uzlom môžu byť oneskorené.
- Hlásenie údajov o výkone a alarmoch v reálnom čase je oneskorené a informácie nie je možné získať včas.
- Spracovanie služby je pomalé, čo spôsobuje hromadenie správ.

Možné príčiny

- Systém je dočasne zaneprázdnený.
- Prah generovania alarmu pre využitie CPU uzla je nevhodný.
- Vykonávajú sa operácie náročné na systémové prostriedky.
- Hardvérový výkon uzla je nízky. Systém preto nemôže fungovať správne.

Postup

1. Prihláste sa do PowerEcho.
 - a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.
-  **NOTE**

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.
- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Skontrolujte , či sa na PowerEcho nevykonáva viacero úloh.

Na PowerEcho vyberte z hlavnej ponuky **System > Task List** , počkajte , kým sa nedokončia všetky úlohy, a potom skontrolujte, či je alarm vymazaný.

 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, prejdite na 3 .
 3. Skontrolujte, či sú prahové hodnoty pre tento alarm vhodné.
 - a. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Threshold Rule Settings**.
 - b. Na navigačnej table vyberte položku **Exception and Event Thresholds**.
 - c. V ľavom hornom rohu stránky **Exception and Event Thresholds** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias** a skontrolujte, či sú prahové hodnoty pre tento alarm vhodné.
 - Ak áno, prejdite na 4.
 - Ak nie, nastavte príslušné prahové hodnoty a prejdite na 7.
 4. Skontrolujte procesy s vysokým využitím CPU v uzle, kde sa generuje alarm.
 - a. Na navigačnej table vyberte položku **Node Monitoring**.
 - b. V ľavom hornom rohu stránky **Node Monitoring** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias**.
 - c. V zozname uzlov kliknite na názov uzla zodpovedajúci hodnote **Host** v parametroch alarmu.

- d. Na karte **Processes** na stránke **Node Details** zoradíte stĺpec **CPU Usage** v zostupnom poradí a skontrolujete, či existujú procesy, ktorých využitie CPU je príliš vysoké.
- Ak áno, zozbierajte predchádzajúce informácie o spracovaní alarmov a kontaktujte technickú podporu.
Skontrolujte, či je alarm vymazaný. Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. Ak alarm pretrváva, prejdite na 5.
 - Ak nie, prejdite na 5.
5. Skontrolujte procesy s vysokým využitím CPU (okrem tých v 4) v uzle, kde sa generuje alarm.
- Použite PuTTY na prihlásenie do chybného uzla uvedeného v detailoch alarmu ako používateľ **sopuser** v režime SSH.
 - Spustíte nasledujúci príkaz a skontrolujete, či existujú procesy, ktorých využitie CPU je vyššie ako pri iných procesoch:
top -o -%CPU
Zobrazia sa informácie podobné nasledujúcim. Hodnoty v stĺpci **%CPU** sa zobrazujú v zostupnom poradí. Stlačte **Ctrl + C**.
- | PID | USER | PR | NI | VIRT | RES | SHR | S | %CPU | %MEM | TIME+ | COMMAND |
|-------|--------|----|----|---------|--------|-------|---|------|------|----------|-----------------|
| 61770 | ossadm | 20 | 0 | 1256940 | 557140 | 14468 | S | 8.6 | 1.7 | 17:41.24 | java |
| 94185 | dbuser | 20 | 0 | 3199468 | 1.2g | 10404 | S | 2.7 | 3.8 | 10:31.46 | zengine |
| 31114 | ossadm | 20 | 0 | 1622324 | 26700 | 11820 | S | 1.0 | 0.1 | 1:35.73 | serviceawarewat |
| 68314 | ossadm | 20 | 0 | 1121276 | 513404 | 13808 | S | 1.0 | 1.6 | 5:11.48 | java |
| ... | | | | | | | | | | | |
- Ak áno, zozbierajte predchádzajúce informácie o spracovaní alarmov a kontaktujte technickú podporu.
Skontrolujte, či je alarm vymazaný. Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. Ak alarm pretrváva, prejdite na 6 .
 - Ak nie, prejdite na 6.
6. Skontrolujte, či hardvérová kapacita požadovaná aktuálnou stupnicou správy prekračuje skutočnú hardvérovú kapacitu servera a či je tento alarm často alebo neustále hlásený.
- Ak áno, výkon hardvéru nemôže spĺňať bežiacie požiadavky systému. Kontaktujte technickú podporu. Nevyžadujú sa žiadne ďalšie kroky.
 - Ak nie, prejdite na 7.
7. Počkajte 1 minútu a potom skontrolujte, či je alarm vymazaný.
- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, zozbierajte predchádzajúce informácie o spracovaní alarmu a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm na PowerEcho, vyberte **Maintenance >**

Operation and Maintenance Management > Exceptions and Events a kliknite na **Clear** v stĺpci **Operation** alarmu nakarte **Exceptions**.

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Verzia operačného systému uzla, pre ktorý sa generuje tento alarm, sa zmenila.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM- 152 Služba OSS je ukončená abnormálne

Popis alarmu

V prípade procesu, ktorý nie je v aktívnom/pohotovostnom režime, ak PowerEcho zistí (detekcia sa vykonáva každých 30 sekúnd), že servisný proces je abnormálny a nepodarí sa ho reštartovať 10-krát za sebou, vygeneruje sa tento alarm. Tento alarm sa automaticky vymaže, keď PowerEcho zistí, že proces beží. V prípade procesu v aktívnom/pohotovostnom režime, ak PowerEcho zistí (detekcia sa vykonáva každých 10 sekúnd), že aktívny proces je abnormálny a nepodarí sa ho reštartovať, vygeneruje sa tento alarm. Tento alarm sa automaticky vymaže, keď PowerEcho zistí, že je spustený aktívny proces alebo sa aktivuje pohotovostný proces.

NOTE

Definícia abnormálneho procesu:

- Pre proces, ktorý nie je v aktívnom/pohotovostnom režime, je proces v stave D (TASK_UNINTERRUPTIBLE) 30-krát za sebou.
- Pre proces v aktívnom/pohotovostnom režime je proces v stave D (TASK_UNINTERRUPTIBLE) 60 krát za sebou.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
152	Major	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Názov servera	Názov chybného uzla.
	SvcAgent	Názov procesu, pre ktorý sa generuje alarm.
	SvcName	Názov inštancie služby, pre ktorú sa generuje alarm.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

Po ukončení procesov sú súvisiace servisné funkcie nedostupné a služby, ktoré závisia od funkcií, nie sú dostupné.

Možné príčiny

Proces sa neočakávane ukončí a nedá sa spustiť, alebo je proces v stave D.

Postup

Získajte **Location Info** alarmu a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm na PowerEcho, vyberte **Maintenance > Operation and Maintenance Management > Exceptions and Events** a kliknite na **Clear** v stĺpci **Operation** alarmu nakarte **Exceptions**

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM- 154 Využitie pamäte je príliš vysoké

Popis alarmu

Tento alarm sa generuje, keď PowerEcho zistí (detekcia sa vykonáva každých 60 sekúnd) , že využitie fyzickej pamäte je väčšie alebo rovné prahu generovania alarmu pre N (N sú časy preťaženia) po sebe idúcich časov. Tento alarm sa automaticky vymaže, keď je využitie fyzickej pamäte menšie ako prah zrušenia alarmu.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
154	Major	Cez limit

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Operačný systém	OS servera.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	Generačný prah	Prahová hodnota pre vygenerovanie alarmu.
	Prahová hodnota	Prahová hodnota pre zrušenie alarmu.
	Použitie	Využitie fyzickej pamäte.
	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

Uzol, pre ktorý sa generuje alarm, reaguje pomaly a operácie súvisiace s uzlom môžu byť oneskorené.

Možné príčiny

- Prah generovania alarmu pre využitie fyzickej pamäte uzla je nevhodný.
- Vykonávajú sa operácie náročné na systémové prostriedky alebo časovo náročné operácie.
- Služby sú zaneprázdnené a využitie pamäte sa zvyšuje.
- Vyskytne sa chyba programu.

Postup

1. Prihláste sa do PowerEcho.
 - a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Skontrolujte, či sú prahové hodnoty pre tento alarm vhodné.
 - a. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Threshold Rule Settings**.
 - b. Na navigačnej table vyberte položku **Exception and Event Thresholds**.
 - c. V ľavom hornom rohu stránky **Exception and Event Thresholds** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias** a skontrolujte, či sú prahové hodnoty pre tento alarm vhodné.
 - Ak áno, prejdite na 3.
 - Ak nie, nastavte príslušné prahové hodnoty a prejdite na 6.
3. Skontrolujte procesy s veľkou veľkosťou použitej fyzickej pamäte na uzle, kde sa generuje alarm.
 - a. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Panoramic Monitoring**.
 - b. Na navigačnej table vyberte položku **Node Monitoring**.
 - c. V ľavom hornom rohu stránky **Node Monitoring** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias**.
 - d. V zozname uzlov kliknite na názov uzla zodpovedajúci hodnote **Host** v parametroch alarmu.
 - e. Na karte **Processes** na stránke **Node Details** zoradte stĺpec **Physical Memory** v zostupnom poradí a skontrolujte, či existujú procesy s veľkou veľkosťou použitej fyzickej pamäte.
 - Ak áno, zozbierajte predchádzajúce informácie o spracovaní alarmov a kontaktujte technickú podporu. Skontrolujte, či je alarm vymazaný. Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. Ak alarm pretrváva, prejdite na 4.
 - Ak nie, prejdite na 4.
4. Skontrolujte procesy s vysokým využitím fyzickej pamäte (okrem procesov v 3) v uzle, kde sa generuje alarm.
 - a. Použite PuTTY na prihlásenie sa do chybného uzla ako používateľ **sopuser** v režime SSH.

- b. Spustíte nasledujúci príkaz a skontrolujete, či existujú procesy, ktorých využitie fyzickej pamäte je vyššie ako pri iných procesoch:

top -o -%MEM

Zobrazia sa informácie podobné nasledujúcim. Hodnoty v stĺpci **%MEM** sú zobrazené v zostupnom poradí. Stlačte **Ctrl + C**.

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
94185	dbuser	20	0	3199468	1.2g	10404	S	3.7	3.8	10:31.79	zengine
68314	ossadm	20	0	1121276	513404	13808	S	3.7	1.6	5:11.63	java
164860	ossadm	20	0	832312	496564	18164	S	20.199	1.539	1480:48	java
...											

- Ak áno, zozbierajte predchádzajúce informácie o spracovaní alarmov a kontaktujte technickú podporu.

Skontrolujte, či je alarm vymazaný. Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. Ak alarm pretrváva, prejdite na 5.

- Ak nie, prejdite na 5.

5. Skontrolujte, či sa využitie fyzickej pamäte uzla stále zvyšuje.

- a. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Panoramic Monitoring**.

- b. Na navigačnej table vyberte položku **Node Monitoring**.

- c. V ľavom hornom rohu stránky **Node Monitoring** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias**.

- d. V zozname uzlov nájdite názov uzla zodpovedajúci **Host** v parametroch alarmu.

- e. Skontrolujte, či sa využitie fyzickej pamäte uzla stále zvyšuje.

- Ak áno, zozbierajte predchádzajúce informácie o spracovaní alarmov a kontaktujte technickú podporu.
- Ak nie, prekonfigurujte prahové hodnoty pre tento alarm na stránke **Threshold Rule Settings** a prejdite na 6.

6. Počkajte 1 minútu a potom skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, zozbierajte predchádzajúce informácie o spracovaní alarmu a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm na Power Echo, vyberte **Maintenance > Operation and Maintenance Management > Exceptions and Events** a kliknite na **Clear** v stĺpci **Operation** alarmu nakarte **Exceptions**.

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Verzia operačného systému uzla, pre ktorý sa generuje tento alarm, sa zmenila.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM-160 Pohotovostné pripojenie k serveru vzdialenej autentifikácie zlyhalo

Popis alarmu

Ak je povolená autentifikácia LDAP a **User authentication mode** je nastavený na možnosť **Fixed user**, SmartPVMS alebo PowerEcho kontroluje pripojenia s aktívnymi a pohotovostnými servermi LDAP v určenom intervale. Interval kontroly je štandardne päť minút. Tento alarm sa generuje, keď je SmartPVMS alebo PowerEcho, že pripojenie k pohotovostnému serveru LDAP je abnormálne. Tento alarm sa automaticky vymaže, keď sa pripojenie k pohotovostnému serveru LDAP stane normálnym.

NOTE

Interval kontroly je možné nastaviť v časti **Server check interval** v **LDAP Authentication** .

1. Vykonajte operácie na základe zdroja alarmu.
 - TheSmartPVMS: Prihláste sa do SmartPVMS .Z hlavnej ponuky vyberte **System > System Management > Authentication**.
 - PowerEcho: Prihláste sa do PowerEcho . Z hlavnej ponuky vyberte **System > Security Management > Authentication**.
2. Na navigačnom paneli vyberte položku **Remote Authentication**.
3. Na stránke **Remote Authentication** kliknite na **LDAP Authentication** .
4. Nastavte **Server check interval**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
160	Kritické	Environmentálny alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	IP servera	Adresa pohotovostného servera LDAP.
Ďalšie informácie	Typ služby	Režim vzdialenej autentifikácie.
	typ produktu	Ak je zdrojom alarmu PowerEcho , tento parameter je uvedený v detailoch alarmu.

Vplyv na systém

Pri autentifikácii LDAP nemôže pohotovostný server LDAP poskytovať službu autentifikácie.

Možné príčiny

- Pohotovostný server LDAP nie je spustený.
- TheSmartPVMS je odpojený od pohotovostného servera LDAP.
- PowerEcho je odpojený od pohotovostného servera LDAP.

Postup

1. Skontrolujte hodnotu **Server IP** v **Location Info** alarmu, ktorá označuje adresu pohotovostného servera LDAP.
2. Skontrolujte, či pohotovostný server LDAP funguje správne.
 - Ak pohotovostný server LDAP funguje správne, prejdite na 3.
 - Ak pohotovostný server LDAP nebeží, spustite pohotovostný server LDAP a prejdite na 5.

NOTE

Server LDAP poskytujú zákazníci na vzdialenú autentifikáciu. Kontaktujte správcu zákazníka, aby skontroloval, či server funguje správne.

3. Skontrolujte, či SmartPVMS je správne pripojený k pohotovostnému LDAP serveru.
 - a. Použite PuTTY na prihlásenie do uzla, kde sídli SMLogLic alebo používateľský proces SM, ako používateľ **sopuser** v režime SSH. Podrobnosti o tom, ako získať adresu IP uzla, v ktorom sa nachádza proces alebo služba, nájdete v časti „Dopyt na adresu IP správy uzla, v ktorom sa nachádza proces alebo služba v *príručke správcu*“.
 - b. Skontrolujte, či je systém správne pripojený k pohotovostnému serveru LDAP.
 - Ak je adresa IP adresou IPv4, spustite nasledujúci príkaz:
ping IP address of the standby LDAP server
 - Ak je adresa IP adresou IPv6, spustite nasledujúci príkaz:
ping6 IP address of the standby LDAP server

Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Stlačením **Ctrl+C** príkaz zastavíte.

```
64 bytes from address of the standby LDAP server
```

Ak sa do 1 minúty nevrátia žiadne informácie, sieťové pripojenie je abnormálne. Stlačením klávesov **Ctrl+C** zastavte príkaz a opravte poruchu siete.

4. Skontrolujte, či je PowerEcho správne pripojené k pohotovostnému serveru LDAP.
 - a. Použite PuTTY na prihlásenie do riadiaceho uzla ako používateľ **sopuser** v režime SSH.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 alebo Management1. Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Querying the Management IP Address of the Node Where a Process or Service Resides“ in *Administrator Guide*.

b. Skontrolujte, či je systém správne pripojený k pohotovostnému serveru LDAP.

- Ak je adresa IP adresou IPv4, spustíte nasledujúci príkaz:

ping *IP address of the standby LDAP server*

- Ak je adresa IP adresou IPv6, spustíte nasledujúci príkaz:

ping6 *IP address of the standby LDAP server*

Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Stlačením **Ctrl+C** príkaz zastavíte.

```
64 bytes from address of the standby LDAP server
```

Ak sa do 1 minúty nevrátia žiadne informácie, sieťové pripojenie je abnormálne. Stlačením klávesov **Ctrl+C** zastavte príkaz a opravte poruchu siete.

5. Počkajte 5 minút a skontrolujte, či je alarm vymazaný.

NOTE

Interval, v ktorom sa alarm vymaže, je rovnaký ako hodnota **Server check interval**. Predvolená hodnota je 5 minút.

- Ak áno, nie sú potrebné žiadne ďalšie kroky.
- Ak nie, získajte informácie o spracovaní alarmov a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-298 Používateľ v skupine SManagers zmení heslo používateľa

Popis alarmu

Tento alarm sa generuje, keď bezpečnostný administrátor zmení heslo iného používateľa.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
298	Kritické	Bezpečnostný alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Používateľské meno	Meno používateľa, ktorého heslo sa zmenilo.
	Časová značka	Čas zmeny hesla používateľa.
Ďalšie informácie	Meno operátora	Meno používateľa, ktorý zmení heslo.

Vplyv na systém

Používateľ vyžaduje na prihlásenie nové heslo, pretože staré heslo bolo po zmene zahodené.

Možné príčiny

Bezpečnostný administrátor zmenil heslo iného používateľa.

Postup

Skontrolujte, či používateľ získal nové heslo. Ak nie, kontaktujte bezpečnostného správcu.

Vymazanie alarmu

ADMC: Po odstránení poruchy musíte tento alarm manuálne vymazať.

ALM-299 Používateľ OSS je pridaný do skupiny správcov, SManagers alebo skupiny správcov zabezpečenia subdomén

Popis alarmu

Tento alarm sa generuje, keď je používateľ pridaný do skupiny **Administrators**, **SManagers** alebo **Subdomain Security Administrator**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
299	Kritické	Bezpečnostný alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Používateľské meno	Meno používateľa, ktorý je pridaný do skupiny Administrators , SManagers alebo Subdomain Security Administrator .
Ďalšie informácie	Meno operátora	Meno používateľa, ktorý pridá ďalšieho používateľa do Administrators , SManagerov alebo Subdomain Security Administrator Group .

Vplyv na systém

Po pridaní používateľa do skupiny **Administrators**, **SManagers** alebo **Subdomain Security Administrator** má tento používateľ všetky povolenia pre túto rolu.

Možné príčiny

- Používateľ je pridaný do skupiny **Administrators**.
- Používateľ je pridaný do skupiny **SManagers**.
- Používateľ je pripojený k skupine **Subdomain Security Administrator Group**.

Postup

Obráťte sa na operátora, aby skontroloval, či je oprávnenie používateľa správne.

Vymazanie alarmu

ADMC: Po odstránení poruchy musíte tento alarm manuálne vymazať.

ALM-1067 Záložné dátové balíky neexistujú

Popis alarmu

PowerEcho skontroluje, či v rámci monitorovacieho obdobia existujú nasledujúce typy záložných balíkov. Tento alarm sa generuje, ak niektorý z nasledujúcich záložných balíkov neexistuje počas nakonfigurovaného časového obdobia.

- Balíky na zálohovanie údajov o produktoch
- Záložné balíky aplikácií produktu
- Záložné balíky databázových aplikácií
- Záložné balíčky operačného systému akéhokoľvek uzla
- Záložné balíčky PowerEcho

Tento alarm sa automaticky vymaže, keď PowerEcho úspešne vykoná úlohu zálohovania zodpovedajúceho typu.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
1067	Menší	Stav zálohy

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
	Stojan č.	Číslo skrine, pre ktorú sa generuje alarm.
	Subrack č.	Číslo podradníka, pre ktorý sa generuje alarm.
	Slot č.	Číslo slotu dosky, pre ktorý sa generuje alarm.
	Dôvod	Možná príčina alarmu.
	Skontrolujte objekt	Objekt, ktorý sa má skontrolovať po vygenerovaní alarmu.

Vplyv na systém

Údaje nie je možné obnoviť.

Možné príčiny

- Údaje nie sú včas zálohované.
- PowerEcho nedokončí vykonávanie úlohy zálohovania.

Postup

1. Prihláste sa do PowerEcho.
 - a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Z hlavnej ponuky vyberte **Backup and Restore > Data Backup**. Vytvorte úlohu zálohovania na základe typu alarmu.
3. Skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy systém automaticky vymaže alarm. Manuálne čistenie nie je potrebné.

ALM-30004 Platnosť hesla používateľa čoskoro vyprší

Popis alarmu

Tento alarm sa generuje, keď je doba platnosti hesla používateľa tretej strany alebo používateľa správcu systému kratšia alebo rovná počtu dní zadaným parametrom **In advance warning before password expires** (predvolene 10 dní). Tento alarm sa automaticky vymaže pri zmene hesla používateľa.

NOTE

- Ak je používateľ správcu systému uzamknutý, tento alarm sa negeneruje, keď sa blíži vypršanie platnosti hesla tohto používateľa.
- Minimálnu zostávajúcu dobu platnosti hesla je možné nastaviť v **Password Policy**.
 1. Vykonajte operácie na základe toho, či je typ produktu obsiahnutý v dodatočných informáciách.
 - Ak nie, alarm je alarm SmartPVMS. V tomto prípade sa prihláste do SmartPVMS. Z hlavnej ponuky vyberte **System > System Management > User Policies**.
 - Ak áno, alarm je alarm PowerEcho. Prihláste sa do PowerEcho a z hlavnej ponuky vyberte **System > Security Management > User Policies**.
 2. Na navigačnej table vyberte položku **Password Policy**.
 3. Nastavte **In advance warning before password expires**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
30004	Major	Alarm v časovej doméne

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Používateľské meno	Meno používateľa, ktorého platnosť hesla čoskoro vyprší.
Ďalšie informácie	typ produktu	Ak je zdrojom alarmu PowerEcho , tento parameter je uvedený v detailoch alarmu.

Vplyv na systém

Ak sa tento alarm nespracuje včas, systém tretej strany alebo správca systému sa po vypršaní platnosti hesla nemôže prihlásiť do systému.

Možné príčiny

- Zostávajúca doba platnosti hesla je menšia alebo rovná hodnote **In advance warning before password expires** nastavenej v **Password Policy**.

- Zostávajúca doba platnosti hesla je menšia alebo rovná hodnote **In advance warning before password expires** nastavenej v rozšírených nastaveniach.

Postup

1. Skontrolujte hodnoty v **Location Info** alarmu a zistite používateľa (používateľa tretej strany alebo správcu systému), ktorého platnosť hesla čoskoro vyprší.
 - Ak je používateľ používateľom tretej strany, prejdite na 2.
 - Ak je používateľ správcom systému, prejdite na 3.
2. Ak chcete obnoviť heslo, kontaktujte správcu bezpečnosti.
 - a. Vykonať operácie na základe zdroja alarmu.
 - Ak používateľ patrí do SmartPVMS: Prihláste sa do SmartPVMS. Z hlavnej ponuky vyberte **System > System Management > User Management**.
 - Ak používateľ patrí do PowerEcho: Prihláste sa do PowerEcho. Z hlavnej ponuky vyberte **System > System Management > User Management**.
 - b. Na navigačnej table vyberte položku **Users**.
 - c. V zozname **Users** kliknite na položku **Reset Password** v stĺpci **Operation** v riadku, ktorý obsahuje používateľa tretej strany, ktorého platnosť hesla čoskoro vyprší a prejdite na bod 4.

NOTE

Po resetovaní hesla pre používateľa tretej strany včas zmeňte heslo používateľa v systéme tretej strany, aby ste zabezpečili prístup do systému tretej strany.

3. Zmeňte heslo pre používateľa správcu systému jedným z nasledujúcich spôsobov:
 - Zmeňte heslo podľa výzvy.
 - a. Ak chcete zmeniť heslo pre používateľa SmartPVMS, prihláste sa do SmartPVMS ako používateľ správcu systému. Ak chcete zmeniť heslo pre používateľa PowerEcho, prihláste sa do PowerEcho ako používateľ správcu systému.
 - b. Zadajte staré heslo a nové heslo, potvrdte nové heslo a kliknite na tlačidlo **Apply**.
 - Zmeňte heslo v **Personal Settings**.
 - a. Vykonať operácie na základe zdroja alarmu.
 - Ak používateľ patrí do SmartPVMS: Prihláste sa do SmartPVMS. Z hlavnej ponuky vyberte **System > System Settings > Personal Settings**.
 - Ak používateľ patrí do PowerEcho: Prihláste sa do PowerEcho. Z hlavnej ponuky vyberte **System > Security Management > Change Password**.
 - b. V dialógovom okne **Change password** zadajte **Old password**, **New password**, a **Confirm password**. Potom kliknite na tlačidlo **Apply**.
4. Počkajte 1 hodinu a skontrolujte, či je alarm vymazaný.

- Ak áno, nie sú potrebné žiadne ďalšie kroky.
- Ak nie, získajte informácie o spracovaní alarmov a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy systém automaticky vymaže alarm. Manuálne čistenie nie je potrebné.

ALM-30005 Platnosť hesla používateľa vypršala

Popis alarmu

Tento alarm sa generuje, keď vyprší platnosť hesla pre používateľa tretej strany alebo správcu systému v systéme. (Štandardne je predvolená doba platnosti 90 dní). Tento alarm sa automaticky vymaže, keď je heslo pre používateľa tretej strany alebo používateľa správcu systému v systéme v rámci doby platnosti.

NOTE

- Ak je používateľ správcu systému uzamknutý, tento alarm sa nevygeneruje, keď vyprší platnosť hesla tohto používateľa.
- Dobu platnosti hesla používateľa je možné nastaviť v **Password Policy**.
 1. Vykonajte operácie na základe toho, či je Typ produktu obsiahnutý v dodatočných informáciách.
 - Ak nie, alarm je alarm SmartPVMS. V tomto prípade sa prihláste do SmartPVMS. Z hlavnej ponuky vyberte **System > System Management > User Policies**.
 - Ak áno, alarm je alarm PowerEcho. Prihláste sa do PowerEcho a z hlavnej ponuky vyberte **System > System Management > User Policies**.
 2. Na navigačnej table vyberte položku **Password Policy**.
 3. Nastavte **Password validity (days)**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
30005	Kritické	Alarm v časovej doméne

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Používateľské meno	Meno používateľa, ktorého platnosť hesla vypršala.
Ďalšie informácie	typ produktu	Ak je zdrojom alarmu PowerEcho , tento parameter je uvedený v detailoch alarmu.

Vplyv na systém

Systém alebo správca systému tretej strany sa nemôže prihlásiť do systému.

Možné príčiny

Platnosť hesla pre používateľa tretej strany alebo používateľa správcu systému vypršala.

Postup

1. Skontrolujte hodnoty v **Location Info** alarmu a zistite používateľa (používateľa tretej strany alebo správcu systému), ktorého heslo vypršalo.
 - Ak je používateľ používateľom tretej strany, prejdite na 2.
 - Ak je používateľ správcom systému, prejdite na 3.
2. Ak chcete obnoviť heslo, kontaktujte správcu bezpečnosti.
 - a. Vykonajte operácie na základe zdroja alarmu.
 - Ak používateľ patrí do SmartPVMS : Prihláste sa do SmartPVMS. Z hlavnej ponuky vyberte **System > System Management > User Management**.
 - Ak používateľ patrí do PowerEcho : Prihláste sa do PowerEcho. Z hlavnej ponuky vyberte **System > Security Management > User Management**.
 - b. Na navigačnej table vyberte položku **Users**.
 - c. V zozname **Users** kliknite na položku **Reset Password** v stĺpci **Operation** v riadku, ktorý obsahuje používateľa tretej strany, ktorého platnosť hesla čoskoro vyprší, a prejdite na 4.

NOTE

Po resetovaní hesla pre používateľa tretej strany včas zmeňte heslo používateľa v systéme tretej strany, aby ste zabezpečili prístup do systému tretej strany.

3. Zmeňte heslo podľa výzvy.
 - a. Ak chcete zmeniť heslo pre používateľa SmartPVMS , prihláste sa do SmartPVMS ako používateľ správcu systému. Ak chcete zmeniť heslo pre používateľa PowerEcho, prihláste sa do PowerEcho ako používateľ správcu systému.
 - b. Zadajte staré heslo a nové heslo, potvrdte nové heslo a kliknite na tlačidlo **Apply**.
4. Počkajte 1 hodinu a skontrolujte, či je alarm vymazaný.
 - Ak áno, nie sú potrebné žiadne ďalšie kroky.
 - Ak nie, získajte informácie o spracovaní alarmov a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy systém automaticky vymaže alarm. Manuálne čistenie nie je potrebné.

ALM-51020 Platnosť certifikátu čoskoro vyprší

Popis alarmu

Systém vykonáva dennú kontrolu doby platnosti certifikátov, ako sú certifikáty ER a IR certifikáty PowerEcho a SmartPVMS a CA certifikáty, certifikáty Syslog, certifikáty správy používateľov, certifikáty dôveryhodnosti SSO, certifikáty LDAP a certifikáty RADIUS PowerEcho. Tento alarm sa generuje, keď je doba platnosti certifikátu kratšia ako 90 dní.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
51020	Major	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	IP adresa uzla, pre ktorý sa generuje alarm.
	Typ certifikátu	Certifikát ER, certifikát CA, certifikát IR, certifikát Syslog, certifikát správy používateľov, certifikát LDAP, certifikát RADIUS, certifikát dôveryhodnosti SSO a ďalšie certifikáty. Ak je alarm vygenerovaný pre iný ako predchádzajúci certifikát, tento parameter obsahuje názov služby, ktorej certifikát patrí.
	Názov služby	Názov inštancie služby SmartPVMS zodpovedajúcej certifikátu.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.

Vplyv na systém

- Ak platnosť certifikátu ER vypršala, nemôžete sa prihlásiť do PowerEcho alebo webového klienta SmartPVMS.
- Ak platnosť certifikátu CA vypršala, správa bezpečnosti IR certifikátu a jeho kľúča je nedostupná.
- Ak platnosť IR certifikátov vyprší, je ovplyvnená interná komunikácia systému.
- Ak platnosť certifikátov Syslog vyprší, protokoly PowerEcho sa nedajú poslať ďalej.
- Ak platnosť certifikátov LDAP vypršala, server LDAP sa nedá pripojiť.

- Ak platnosť certifikátov RADIUS vypršala, server RADIUS sa nedá pripojiť.
- Ak platnosť dôveryhodného certifikátu SSO vyprší, prihlásenie do klienta SSO zlyhá.

Možné príčiny

Doba platnosti certifikátu je kratšia ako 90 dní.

Postup

Na základe typu certifikátu v informáciách o umiestnení manuálne aktualizujte certifikát podľa tabuľky1.

Tabuľka 1 Návod na obsluhu	
Typ certifikátu	Prevádzka
ER certifikát	Podrobnosti nájdete v časti „Uploading and Updating ER Certificates“ v <i>Administrator Guide</i> .
Certifikáty CA	Podrobnosti nájdete v časti „Uploading and Updating Certificates of the PowerEcho for Internal SmartPVMS Communication“ v <i>Administrator Guide</i> .
Certifikát Syslog	Podrobnosti nájdete v časti „Uploading and Updating the PowerEcho Certificates for Communication Between SmartPVMS and Third-Party Systems“ v <i>Administrator Guide</i> .
Certifikát dôveryhodnosti SSO	
IR certifikát	Podrobnosti nájdete v časti „Updating IR Certificates“ v <i>Administrator Guide</i> .
Certifikát správy používateľov	Podrobnosti nájdete v časti „Updating User Management Certificates of the PowerEcho“ v <i>Administrator Guide</i> .
LDAP certifikát PowerEcho	Podrobnosti nájdete v časti „Updating LDAP Certificates of the PowerEcho“ v <i>Administrator Guide</i> .
RADIUS certifikát PowerEcho	Podrobnosti nájdete v časti „Updating RADIUS Certificates of the PowerEcho“ v <i>Administrator Guide</i> .
Iné certifikáty	Ak chcete získať spôsob aktualizácie certifikátu, vyhľadajte názov služby uvedený v časti Informácie o type Certificate Type of Location Info v časti „Certificate List“ v <i>Administrator Guide</i> .

Vymazanie alarmu

ADAC: Systém skontroluje platnosť certifikátu o 00:00:00 po aktualizácii certifikátu. Ak je certifikát platný, tento alarm sa automaticky zruší.

ALM-51021 Platnosť certifikátu vypršala

Popis alarmu

Systém vykonáva dennú kontrolu doby platnosti certifikátov, ako sú ER certifikáty PowerEcho a SmartPVMS a certifikáty Syslog, certifikáty LDAP, certifikáty RADIUS, certifikáty správy používateľov a certifikáty dôveryhodnosti SSO PowerEcho. Tento alarm sa generuje po vypršaní platnosti certifikátu.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
51021	Kritické	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	IP adresa uzla, pre ktorý sa generuje alarm.
	Typ certifikátu	Certifikát ER, certifikát Syslog, certifikát správy používateľov, certifikát LDAP, certifikát RADIUS, certifikát dôveryhodnosti SSO a ďalšie certifikáty. Ak je alarm vygenerovaný pre iný ako predchádzajúci certifikát, tento parameter obsahuje názov služby, ktorej certifikát patrí.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.

Vplyv na systém

- Ak platnosť certifikátu ER vypršala, nemôžete sa prihlásiť do PowerEcho alebo webového klienta SmartPVMS .
- Ak platnosť certifikátov Syslog vyprší, protokoly PowerEcho sa nedajú poslať ďalej.
- Ak platnosť certifikátov LDAP vypršala, server LDAP sa nedá pripojiť.
- Ak platnosť certifikátov RADIUS vypršala, server RADIUS sa nedá pripojiť.
- Ak platnosť dôveryhodného certifikátu SSO vyprší, prihlásenie do klienta SSO zlyhá.

Možné príčiny

Platnosť certifikátu vypršala.

Postup

Na základe typu certifikátu v informáciách o umiestnení manuálne aktualizujte certifikát podľa tabuľky1.

Tabuľka 1 Návod na obsluhu	
Typ certifikátu	Prevádzka
ER certifikát	Podrobnosti nájdete v časti „Uploading and Updating ER Certificates“ v <i>Administrator Guide</i> .
Certifikát Syslog	Podrobnosti nájdete v časti „Uploading and Updating the PowerEcho Certificates for Communication Between SmartPVMS and Third-Party Systems“ v <i>Administrator Guide</i> .
Certifikát dôveryhodnosti SSO	
Certifikát správy používateľov	Podrobnosti nájdete v časti „Updating User Management Certificates of the PowerEcho“ v <i>Administrator Guide</i> .
LDAP certifikát PowerEcho	Podrobnosti nájdete v časti „Updating LDAP Certificates of the PowerEcho“ v <i>Administrator Guide</i> .
RADIUS certifikát PowerEcho	Podrobnosti nájdete v časti „Updating RADIUS Certificates of the PowerEcho“ v <i>Administrator Guide</i> .
Iné certifikáty	Ak chcete získať spôsob aktualizácie certifikátu, vyhľadajte názov služby uvedený v časti Informácie o type Certificate Type of Location Info v časti „Certificate List“ v <i>Administrator Guide</i> .

Vymazanie alarmu

ADAC: Systém skontroluje platnosť certifikátu o 00:00:00 po aktualizácii certifikátu. Ak je certifikát platný, tento alarm sa automaticky zruší.

ALM-51022 Aktualizácia certifikátu zlyhala

Popis alarmu

Tento alarm sa generuje, keď sa nepodarilo aktualizovať certifikáty ER alebo certifikáty IR v režime CLI.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
51022	Kritické	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Typ certifikátu	ER certifikát alebo IR certifikát.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.

Vplyv na systém

Systém sa nedá prihlásiť alebo je nedostupný.

Možné príčiny

Nový certifikát nespĺňa požiadavky.

Postup

1. Manuálne obnovte certifikáty.
 - Certifikáty ER nájdete v časti „Restoring ER Certificates That Failed to Be Updated“ v *Administrator Guide*.
 - Informácie o certifikátoch IR nájdete v časti „Updating IR Certificates“ v *Administrator Guide*.
2. Skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po aktualizácii certifikátu sa tento alarm automaticky vymaže.

ALM-51023 abnormálna služba NTP

Popis alarmu

PowerEcho predvolene kontroluje nasledujúce položky každých 5 minút . Tento alarm sa generuje, keď PowerEcho zistí , že server NTP existuje, ale neprejaví sa, alebo keď časový rozdiel trikrát po sebe prekročí prahovú hodnotu (predvolene 60 sekúnd).

- Stav serverov NTP
- Maximálny časový rozdiel medzi produktovými uzlami
- Časový rozdiel medzi uzlom a serverom NTP

Tento alarm sa automaticky vymaže, keď PowerEcho zistí , že existujúce servery NTP sú normálne a časový rozdiel nie je väčší ako prahová hodnota pre tri po sebe idúce časy. PowerEcho hlási alarmy rôznej závažnosti na základe scenára poruchy. Napríklad, ak je **Other Information Disconnected NTP address** alebo **Reachable but time synchronization failed NTP address**, ohlásí sa veľký alarm.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
51023	Kritický/hlavný	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Názov uzla	Názov uzla, pre ktorý sa generuje alarm.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.
Ďalšie informácie	NTP adresu	IP adresa abnormálneho servera NTP.
	IP adresa uzla	IP adresa uzla zodpovedajúca maximálnemu časovému rozdielu.
	Časový posun	Maximálny časový rozdiel medzi uzlami produktu alebo časový rozdiel medzi uzlom a serverom NTP.
	Odpojená adresa NTP	IP adresa NTP servera, ktorý je odpojený od uzla.
	Dostupný, ale synchronizácia času zlyhala na adrese NTP	IP adresa servera NTP, ku ktorému sa môže uzol pripojiť, ale nedokáže z neho synchronizovať čas.

Vplyv na systém

Ak SmartPVMS služby nedokážu synchronizovať čas zo servera NTP vyššej vrstvy, čas každého zariadenia v sieti môže byť nepresný. Keď sa vykonávajú operácie vyžadujúce záznam časovej pečiatky, ako je zálohovanie a obnova a záznam prevádzkového protokolu, efektívnosť spracovania služby môže byť ovplyvnená nesprávnou obnovou záložného balíka alebo chybami pri získavaní protokolu.

Možné príčiny

- Vzťah časovej synchronizácie medzi uzlami je abnormálny.
- Čas medzi servermi NTP je nekonzistentný.
- Služba NTP uzla je abnormálna. Konfiguračný súbor NTP alebo proces NTP môžu byť abnormálne alebo čas medzi servermi NTP je nekonzistentný.
- Servery NTP sú abnormálne.
- Komunikácia medzi uzlom a serverom NTP je abnormálna.
- Maximálny časový rozdiel medzi produktovými uzlami presahuje prah.
- Časový rozdiel medzi uzlom a serverom NTP prekračuje prahovú hodnotu.

Postup

Pozrite si možné príčiny alarmu. Skontrolujte možné príčiny alarmu a vyberte zodpovedajúci postup manipulácie podľa tabuľky 1.

Tabuľka 1 Návod na obsluhu

Kategória	Možná príčina	Postup opravy
Služba NTP je abnormálna.	Vzťah časovej synchronizácie medzi uzlami je abnormálny.	<ol style="list-style-type: none">1. Prihláste sa do PowerEcho.<ol style="list-style-type: none">a. Prístup k PowerEcho získate na https://client IP address of the PowerEcho:31945.<p>POZNÁMKA: Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.</p><ol style="list-style-type: none">b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo Log In.2. Na PowerEcho vyberte z hlavnej ponuky Maintenance > Time Management > Configure NTP. Na stránke Configure NTP kliknite na Reconfigure, aby ste obnovili vzťahy synchronizácie času. Skontrolujte, či je alarm vymazaný.<ul style="list-style-type: none">• Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.• Ak alarm pretrváva, kontaktujte technickú podporu.

Tabuľka 1 Návod na obsluhu

Kategória	Možná príčina	Postup opravy
	<p>Čas medzi servermi NTP je nekonzistentný.</p>	<p>Upravte čas servera NTP, aby ste zabezpečili konzistentnosť času medzi servermi NTP. Skontrolujte, či je alarm vymazaný.</p> <ul style="list-style-type: none"> • Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. • Ak alarm pretrváva, kontaktujte technickú podporu .
	<p>Služba NTP uzla je abnormálna. Konfiguračný súbor NTP alebo proces NTP môžu byť abnormálne alebo čas medzi servermi NTP je nekonzistentný.</p>	<ol style="list-style-type: none"> 1. Použijete PuTTY na prihlásenie do uzla, pre ktorý sa generuje alarm v režime SSH ako používateľ sopuser . Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Dopyt na adresu IP správy uzla“ v príručke správcu. 2. Ak chcete prepnúť na používateľa ossadm, spustíte nasledujúci príkaz: > su - ossadm Password: <i>password for the ossadm user</i> 3. Skontrolujte komponent používaný službou NTP: <ul style="list-style-type: none"> • Ak sa pre riadiaci uzol vygeneruje alarm, spustíte nasledujúci príkaz: > <i>installation</i> <i>directory/manager/var/etc/common/custom.cfg grep MGMT_NTP_TYPE</i> Ak sa zobrazia informácie podobné nasledujúcim, služba NTP používa ntpd. Ak sa nezobrazí žiadny výstup príkazu, vykonajte operácie v nasledujúcom scenári. MGMT_NTP_TYPE=ntpd <p>POZNÁMKA: Ak je PowerEcho nasadené v režime klastra, predchádzajúci príkaz je potrebné vykonať na Management0 aj Management1.</p> <ul style="list-style-type: none"> • Ak sa alarm vygeneruje pre produktový uzol alebo jeden z riadiacich uzlov okrem Management0 a Management1, spustíte nasledujúci príkaz: > bash /usr/local /osconfig/os/bin/getsupportntptype.sh <ul style="list-style-type: none"> • Ak sa zobrazia informácie podobné nasledujúcim, operačný systém podporuje ntpd a služba NTP používa ntpd: ["ntpd"]

Tabuľka 1 Návod na obsluhu

Kategória	Možná príčina	Postup opravy
		<ul style="list-style-type: none"> • Ak sa zobrazia informácie podobné nasledujúcim, operačný systém podporuje chrony a služba NTP používa chrony: <pre>["chrony"]</pre> • Ak sa zobrazia informácie podobné nasledujúcim, operačný systém podporuje ntpd a chrony a služba NTP prednostne používa chrony: <pre>["ntpd", "chrony"]</pre> <p>4. Skontrolujte, či je spustená služba NTP, na základe typu komponentu získaného v 3.</p> <ul style="list-style-type: none"> • Ak sa používa komponent ntpd, spustite nasledujúci príkaz: > service ntpd status <ul style="list-style-type: none"> • Ak výstup príkazu obsahuje active (spustený), služba NTP na uzle je spustená. • V opačnom prípade nebude služba NTP na uzle spustená. Prejdite na 5. • Ak sa používa komponent chrony, spustite nasledujúci príkaz: > service chronyd status <ul style="list-style-type: none"> • Ak výstup príkazu obsahuje active (spustený), služba NTP na uzle je spustená. • V opačnom prípade nebude služba NTP na uzle spustená. Prejdite na 5. <p>5. Spustite službu NTP.</p> <ul style="list-style-type: none"> • Ak chcete prepnúť na používateľa root, spustite nasledujúci príkaz: > su - root <pre>Password: password for the root user</pre> • Spustite nasledujúci príkaz na spustenie služby NTP: • Ak sa používa komponent ntpd, spustite nasledujúci príkaz: # service ntpd start • Ak sa používa komponent chrony, spustite nasledujúci príkaz: # systemctl start chronyd

Tabuľka 1 Návod na obsluhu

Kategória	Možná príčina	Postup opravy
		<ul style="list-style-type: none"> • Spustíte nasledujúci príkaz na ukončenie od používateľa root: # exit <p>1. Vykonajte nasledujúce operácie na základe typu komponentu získaného v bode 3. Skontrolujte časový rozdiel medzi aktuálnym uzlom a jeho nadradeným serverom NTP, aby ste určili, či sa má vynútené synchronizovať časové pásmo a čas.</p> <ul style="list-style-type: none"> • Ak sa používa komponent <code>ntpd</code>, spustíte nasledujúci príkaz: > ntpq -np <pre data-bbox="786 775 1548 864">remote ... offset jitter ===== * x.x.x.x ... -0.024 0.043</pre> <p>Ak je absolútna hodnota offset vo výstupe príkazu väčšia ako 5000, časový rozdiel medzi aktuálnym uzlom a serverom NTP vyššej úrovne presiahne 5 sekúnd. V opačnom prípade prejdite na 5.</p> <ul style="list-style-type: none"> • Ak sa používa komponent chrony, spustíte nasledujúci príkaz: > chronyc tracking <pre data-bbox="786 1182 1548 1272">... System time: 8.829101562 seconds fast of NTP time ...</pre> <p>Ak je absolútna hodnota System time vo výstupe príkazu väčšia ako 5 sekúnd, časový rozdiel medzi aktuálnym uzlom a serverom NTP vyššej úrovne presiahne 5 sekúnd. V opačnom prípade prejdite na 5.</p> <p>2. Prihláste sa do PowerEcho.</p> <ul style="list-style-type: none"> • Prístup k PowerEcho získate na https://client IP address of the PowerEcho:31945. <div data-bbox="786 1615 1540 1758" style="background-color: #ffffcc; padding: 5px;"> <p>POZNÁMKA: Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.</p> </div> <ul style="list-style-type: none"> • Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo Log In. <p>3. Na PowerEcho vyberte z hlavnej ponuky Maintenance > Time Management > Configure NTP. Na stránke Configure NTP zmeňte hodnotu Key Index a Key servera NTP na základe zobrazených pravidiel. V opačnom prípade tento krok preskočte.</p>

Tabuľka 1 Návod na obsluhu

Kategória	Možná príčina	Postup opravy
		<p>4. Nútne synchronizuje časové pásmo a čas.</p> <ul style="list-style-type: none"> • Na PowerEcho vyberte z hlavnej ponuky Maintenance > Time Management > Configure Time Zone and Time. • Na stránke Configure Time Zone and Time kliknite na položku Forcibly Synchronize. <p>POZNÁMKA:</p> <ul style="list-style-type: none"> • Pred vynútenou synchronizáciou časového pásma a času PowerEcho automaticky zastaví produktové služby a produktové databázy. V dôsledku toho sú služby nedostupné. Po vynútenej synchronizácii časového pásma a času systém automaticky spustí databázy produktov a produktové služby a funkcie sa sprístupnia. • Na PowerEcho vyberte System > Task list z hlavnej ponuky. Počkajte, kým sa nedokončí úloha nútenej synchronizácie časového pásma a času. • Po vynútenej synchronizácii časového pásma a času počkajte približne 1 až 15 minút a prejdite na 6. <p>5. Upravte čas servera NTP, aby ste zabezpečili konzistentnosť času medzi servermi NTP.</p> <p>6. Skontrolujte, či je alarm vymazaný.</p> <ul style="list-style-type: none"> • Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. • Ak alarm pretrváva, kontaktujte technickú podporu.
	<ul style="list-style-type: none"> • Servery NTP sú abnormálne. • Komunikácia medzi uzlom a serverom NTP je abnormálna. 	<p>1. Skontrolujte, či je sieť medzi riadiacim uzlom a serverom NTP normálna.</p> <p>a. Použite PuTTY na prihlásenie do riadiaceho uzla ako používateľ sopuser v režime SSH.</p> <p>POZNÁMKA: Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 alebo Management1.</p> <p>b. Skontrolujte, či je spojenie so serverom NTP normálne.</p> <p>> su - root</p> <pre> Password: password for the root user # ntpdate -q IP addressa NTP server </pre>

Tabuľka 1 Návod na obsluhu

Kategória	Možná príčina	Postup opravy
		<p>Zobrazia sa informácie podobné nasledujúcim. Ak je hodnota stratum číslo od 1 do 15 a hodnoty offset aj delay nie sú 0, spojenie so serverom NTP je normálne. V opačnom prípade kontaktujte technickú podporu.</p> <pre data-bbox="699 501 1509 555">server IP address of the NTP server, stratum 6, offset -0.000010, delay 0.02599</pre> <ol style="list-style-type: none"> <li data-bbox="746 564 1509 672">c. Spustíte nasledujúci príkaz na ukončenie od používateľa root : # exit <li data-bbox="651 698 1401 770">2. Skontrolujte, či je server NTP normálny. Ak je server NTP abnormálny, opravte poruchu. <li data-bbox="651 797 1541 990">3. Po odstránení poruchy počkajte 30 minút a skontrolujte, či je alarm vymazaný. <ol style="list-style-type: none"> <li data-bbox="746 896 1541 931">a. Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. <li data-bbox="746 958 1445 990">b. Ak alarm pretrváva, kontaktujte technickú podporu.
<p>Je tam časový rozdiel.</p>	<p>Maximálny časový rozdiel medzi produktovými uzlami presahuje prah.</p> <p>Časový rozdiel medzi uzlom a serverom NTP prekračuje prahovú hodnotu.</p>	<ol style="list-style-type: none"> <li data-bbox="651 1039 1509 1272">1. Nútne synchronizuje časové pásmo a čas. <ol style="list-style-type: none"> <li data-bbox="746 1102 1509 1173">a. Na PowerEcho vyberte z hlavnej ponuky Maintenance > Time Management > Configure Time Zone and Time. <li data-bbox="746 1200 1445 1272">b. Na stránke Configure Time Zone and Time kliknite na položku Forcibly Synchronize. <div data-bbox="756 1294 1544 1617" style="background-color: #ffffcc; padding: 5px;"> <p>POZNÁMKA:</p> <ul style="list-style-type: none"> <li data-bbox="788 1335 1509 1576">Pred vynútenou synchronizáciou časového pásma a času PowerEcho automaticky zastaví produktové služby a produktové databázy. V dôsledku toho sú služby nedostupné. Po vynútenej synchronizácii časového pásma a času systém automaticky spustí databázy produktov a produktové služby a funkcie sa sprístupnia. </div> <ol style="list-style-type: none"> <li data-bbox="746 1621 1445 1729">c. Na PowerEcho vyberte System > Task List z hlavnej ponuky. Počkajte, kým sa nedokončí úloha nútenej synchronizácie časového pásma a času. <li data-bbox="651 1756 1541 1948">2. Po vynútenej synchronizácii časového pásma a času počkajte 1 až 15 minút a skontrolujte, či je alarm vymazaný. <ul style="list-style-type: none"> <li data-bbox="746 1854 1541 1890">Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. <li data-bbox="746 1917 1445 1948">Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Tento alarm sa automaticky vymaže, keď PowerEcho zistí, že existujúce servery NTP sú normálne a časový rozdiel nie je väčší ako prahová hodnota pre tri po sebe idúce servery.

ALM-51024 Stav stránky je abnormálny

Popis alarmu

Tento alarm sa generuje, keď systém DR trikrát za sebou (čas detekcie je 30 sekúnd) deteguje, že stav DR produktov na aktívnom mieste a pohotovostnom mieste je abnormálny, to znamená, že produkty na dvoch miestach sú chybné, alebo sú aktívne alebo v pohotovostnom režime. Tento alarm sa automaticky vymaže, ak sa stav lokality stane normálnym.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
51024	Kritické	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Strana 1	Názov strany.
	Alias produktu 1	Produktový alias stránky.
	Strana 2	Názov strany.
	Alias produktu 2	Produktový alias stránky.

Vplyv na systém

- Údaje sú nekonzistentné a nie je možné ich synchronizovať medzi aktívnou lokalitou a pohotovostnou lokalitou.
- Dáta na aktívnom mieste av pohotovostnom režime sa môžu stratiť.

Možné príčiny

- Riadiaci uzol na aktívnej lokalite alebo pohotovostnej lokalite je vypnutý.
- Stav srdcového tepu medzi aktívnym miestom a miestom pohotovostného režimu je abnormálny.
- Služba DR je reštartovaná alebo abnormálna.
- PowerEcho vytvára alebo odstraňuje vzťah DR produktu.
- Produkt na pohotovostnom mieste prevezme služby a prepne sa do aktívneho stavu, keď je stav srdcového tepu medzi aktívnym miestom a pohotovostným miestom abnormálny. V tomto prípade je systém v duálnom aktívnom stave.

- Produkt na aktívnom mieste sa prepne do pohotovostného režimu, keď je stav srdcového tepu medzi aktívnym miestom a miestom pohotovosti abnormálny. V tomto prípade je systém v režime duálneho pohotovostného režimu.
- Stránka sa neaktivuje alebo sa neaktivuje v pohotovostnom režime.

Postup

1. Poruchu odstráňte podľa nasledujúcej tabuľky.

NOTE

Táto časť poskytuje iba základné metódy riešenia problémov. Ak porucha pretrváva aj po odstránení problémov pomocou tejto metódy, kontaktujte technickú podporu.

Tabuľka 1 Skontrolujte položky


Skontrolujte položku	Skontrolujte metódu	Riešenie
Skontrolujte, či je riadiaci uzol na aktívnej lokalite alebo pohotovostnej lokalite vypnutý.	-	<ol style="list-style-type: none"> 1. Kontaktujte správcu, aby skontroloval a zapol VM. 2. Vykonajte operácie na základe scenára. <ul style="list-style-type: none"> • Ak je riadiaci uzol na jednom mieste vypnutý, prejdite na 7 po zapnutí uzla. • Ak sú riadiace uzly na aktívnej lokalite a pohotovostnej lokalite vypnuté, vykonajte 2 až 7 po zapnutí uzlov.
Skontrolujte, či stav srdcového tepu a služby DR medzi aktívnou lokalitou a lokalitou v pohotovostnom režime fungujú správne.	<ul style="list-style-type: none"> • Skontrolujte sieť srdcového tepu medzi aktívnym miestom a miestom v pohotovostnom režime. • Skontrolujte stav služby DR riadiacich uzlov na aktívnej lokalite a lokalite v pohotovostnom režime. • Skontrolujte, či sa systémové certifikáty DR riadiacich uzlov na aktívnej lokalite a lokalite v pohotovostnom režime zhodujú, alebo či im nevypršala platnosť. 	Podrobnosti nájdete v ALM-101201 Abnormal Heartbeat.

Tabuľka 1 Skontrolujte položky

Skontrolujte položku	Skontrolujte metódu	Riešenie
Skontrolujte, či bol vzťah DR produktu úspešne vytvorený alebo odstránený.	Na PowerEcho vyberte System > Tak List z hlavnej ponuky. Na zobrazenej stránke zobrazte stav úlohy.	<ul style="list-style-type: none"> • Ak je úloha úspešne vykonaná, prejdite na 7. • Ak sa úloha nepodarí vykonať, kontaktujte technickú podporu.
Skontrolujte, či sú obe lokality aktívnou stránkou.	Na PowerEcho vyberte z hlavnej ponuky HA > Remote High Availability System > Manage DR System . Na zobrazenej stránke zobrazte stav lokality.	<ul style="list-style-type: none"> • Ak je jedna z lokalít aktívna a druhá pohotovostná , prejdite na 7. • Ak sú obe lokality aktívne, vykonajte 2 až 7.
Skontrolujte, či sa stránka úspešne aktivuje alebo je v pohotovostnom režime.	Na PowerEcho vyberte System > Task z hlavnej ponuky. Na zobrazenej stránke zobrazte stav úlohy.	<ul style="list-style-type: none"> • Ak je úloha úspešne vykonaná, prejdite na 7. • Ak sa úloha nepodarí vykonať, kontaktujte technickú podporu.


2. Prihláste sa do PowerEcho jednej zo stránok.


- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

3. Na PowerEcho vyberte z hlavnej ponuky **HA > Remote High Availability System > Manage DR System**.
4. V stĺpci **Operation** v riadku, ktorý obsahuje produkt s údajmi, ktoré sa majú synchronizovať, kliknite na  . Vyberte smer synchronizácie údajov o produkte.

 **NOTE**

- Ak stavy primárnej lokality a sekundárnej lokality nepozostávajú z jedného aktívneho a jedného pohotovostného stavu, musíte zadať smer synchronizácie údajov o produkte a systém DR vykoná úplnú synchronizáciu na základe zadaného smeru. Napríklad, ak

je určený smer z lokality A do lokality B, údaje lokality B sa prepíšu a údaje správy používateľov PowerEcho lokality B sa prepíšu údajmi lokality A o 00:00:00 hod. nasledujúci deň. Odporúčame vám špecifikovať produkt s najnovšími údajmi ako produkt aktívnej lokality, aby ste z neho synchronizovali údaje s produktom rovnocennej lokality.

- Ak je jedna z primárnej lokality a sekundárnej lokality aktívna a druhá je v pohotovostnom režime, nemusíte špecifikovať smer synchronizácie údajov o produkte. Systém automaticky synchronizuje údaje z aktívnej lokality do pohotovostnej lokality. Údaje o správe používateľov PowerEcho pohotovostnej lokality budú prepísané údajmi aktívnej lokality o 00:00:00 nasledujúceho dňa.

5. Vykonať operácie podľa pokynov.
6. Skontrolujte výsledok operácie. Ak výsledok operácie nie je taký, ako sa očakávalo, kontaktujte technickú podporu.
 - a. Na PowerEcho vyberte z hlavnej ponuky **HA > Remote High Availability System > Manage DR System**.
 - b. Skontrolujte, či je stav srdcového tepu medzi aktívnym miestom a miestom v pohotovostnom režime  .
 - c. Skontrolujte, či je **Data Synchronization Status** všetkých produktov **Synchronized** alebo **Synchronizing** . Ak je **Data Synchronization Status Delayed**, medzi aktívnou lokalitou a pohotovostnou lokalitou sa synchronizuje veľké množstvo údajov . Po dokončení synchronizácie údajov skontrolujte stav.
 - d. Overte si, že sa môžete prihlásiť do SmartPVMS aktívnej stránky.
7. Skontrolujte, či je alarm vymazaný.
 - Ak áno, nie sú potrebné žiadne ďalšie kroky.
 - Ak nie, zozbierajte informácie o manipulácii s alarmom a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-51025 Platnosť certifikátu vzdialeného systému DR vypršala

Popis alarmu

Systém denne kontroluje dobu platnosti certifikátov systému DR . Tento alarm sa generuje, keď doba platnosti certifikátov DR vypršala alebo je neplatná. Tento alarm sa automaticky vymaže po aktualizácii certifikátov systému DR.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
51025	Kritické	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Miesto 1	Typ lokality.
	Miesto 2	Typ lokality.

Vplyv na systém

Ak platnosť certifikátov DR vyprší, komunikácia medzi aktívnou lokalitou a pohotovostnou lokalitou zlyhá po reštarte služby DR.

Možné príčiny

Platnosť certifikátov systému DR vypršala.

Postup

1. Aktualizujte systémový certifikát DR . Podrobnosti nájdete v časti „Updating Certificates for DR System Communication“ v *Administrator Guide*.
2. Skontrolujte, či je alarm vymazaný.
 - Ak áno, nie sú potrebné žiadne ďalšie kroky.
 - Ak nie, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-51026 Certifikát vzdialeného systému DR čoskoro skončí

Popis alarmu

Ak do doby certifikátov systému DR zostáva menej ako 90 dní, systém DR každý deň hlási alarm s blížiacim sa uplynutím platnosti certifikátu. Tento alarm sa automaticky vymaže po aktualizácii certifikátov systému DR.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
51026	Major	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	stránky	Názov lokality.

Vplyv na systém

Komunikácia medzi aktívnym miestom a pohotovostným miestom bude abnormálna.

Možné príčiny

Platnosť certifikátu systému DR vyprší za menej ako 90 dní.

Postup

1. Aktualizujte systémový certifikát DR . Podrobnosti nájdete v časti „Updating Certificates for DR System Communication v *Administrator Guide*.
2. Skontrolujte, či je alarm vymazaný.
 - Ak áno, nie sú potrebné žiadne ďalšie kroky.
 - Ak nie, kontaktujte technickú podporu .

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-51027 Preťaženie dokumentov

Popis alarmu

Informačné centrum štandardne podporuje maximálne 10 GB (10 240 MB) dokumentov. Tento alarm sa generuje, keď je veľkosť dokumentov načítaných do Informačného centra väčšia ako 10 GB.

Ak je nakonfigurovaná veľkosť dokumentov, ktoré je možné načítať, tento alarm sa vygeneruje, keď celková veľkosť dokumentov načítaných do Informačného centra prekročí nakonfigurovanú hodnotu.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
51027	Menší	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Dôvod alarmu	Príčina alarmu.
Ďalšie informácie	Zdrojový systém	Modul, kde je hlásená chyba.
	Návrh na opravu	Alternatívne riešenia alebo opatrenia, ktoré možno prijať.

Vplyv na systém

Keď veľkosť dokumentov prekročí prahovú hodnotu, systém automaticky zastaví načítanie mediačných dokumentov zariadenia, ktoré presahujú maximálnu veľkosť, kým celková veľkosť dokumentov nebude menšia ako nakonfigurovaná hodnota. Dokumenty, ktoré sa nepodarilo načítať, nie je možné prehľadávať ani vyhľadávať.

Keď sa celková veľkosť dokumentov zmenší na špecifikovanú mierku, nevložené mediačné dokumenty zariadenia sa automaticky znova zavedú.

Systémové akcie

žiadne

Možné príčiny

Kategória príčiny	Možná príčina
Konfigurácia údajov	Načíta sa veľký počet dokumentov sprostredkovania zariadenia, čo presahuje rozsah správy dokumentácie nakonfigurovaný počas nasadenia. (Predvolená miera správy dokumentácie Informačného centra je 10 GB.)
softvér	žiadne
Hardvér	žiadne
Iné problémy	žiadne

Postup

1. Odištalujte nepotrebné sprostredkovanie. Podrobnosti o vplyve odištalovania sprostredkovania nájdete v ľavom hornom rohu online pomocníka v hľadanom výraze „**Uninstalling the Mediation**“ a vo výsledku vyhľadávania si pozrite podrobnosti.
2. 10 minút po odištalovaní sprostredkovania vykonajte nasledujúce operácie, aby ste skontrolovali veľkosť dokumentov južných zariadení:
 - a. Použite PuTTY na prihlásenie do uzla, kde sídli ICSService, ako používateľ **sopuser** v režime SSH a získajte cestu k denníku služby. Podrobnosti o tom, ako získať adresu IP uzla, v ktorom sa nachádza služba, nájdete v časti „How Do I Query the IP Address of the Node Where a Service Resides?“ v *Administrator Guide*.

ps -ef |grep ICSService

```
ossuser 124598      1   9 Oct25 ?           02:39:44 /opt/cloud/envs/Product-  
ICSService/20201025055139108/rtsp/jre//bin/java  
-Dlog4j.configurationFile=/opt/cloud/envs/Product-  
ICSService/20201025055139108/rtsp/tomcat/conf/log4j2.xml -  
Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -  
Dfile.encoding=UTF-8  
-Dlog.dir=/var/log/oss/MAE/ICSService/icsservice-3-0 -  
DREQUEST_MAXBODYSIZE=204800 -DNFW=icsservice-3-0 -  
Dorg.apache.catalina.connector.RECYCLE_FACADES=true  
-Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -  
Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true -  
XX:+CrashOnOutOfMemoryError  
-XX:ErrorFile=/var/log/oss/MAE/ICSService/icsservice-3-  
0/logs/dump/hs_err_pid%p.log
```

NOTE

Ako je uvedené v predchádzajúcom príklade, cesta protokolu Informačného centra je **/var/log/oss/ MAE /ICSService/ icsservice-3-0** . Vymeňte ho na základe požiadaviek lokality.

- b. Spustíte nasledujúci príkaz, aby ste skontrolovali hodnotu **south libData totalSize** v súbore **root.log**:

```
grep "south libData totalSize" /var/log/oss/ MAE /ICSService/ icsservice-3-0 /log/root.log
```

Nahradíte **/var/log/oss/ MAE /ICSService/ icsservice-3-0** cestou získanou v 2.a.

```
2020-10-25 12:33:20,603 WARN [pool-16-thread-1][LibDataPathFilter.java 71]
south libData totalSize: 12369M
2020-10-25 14:08:20,532 WARN [pool-16-thread-1][LibDataPathFilter.java 71]
south libData totalSize: 14138M
2020-10-26 10:33:20,601 WARN [pool-16-thread-1][LibDataPathFilter.java 71]
south libData totalSize: 9174M
```

Vo výstupe príkazu je hodnota **south libData totalSize** k poslednému dátumu celková veľkosť dokumentov zariadenia na juh v systéme. V predchádzajúcom príklade je hodnota 9 174 MB, čo je menej ako celková veľkosť dokumentov, ktoré je možné načítať (predvolená hodnota je 10 240 MB). V tomto prípade prejdite na 3.

NOTE

Ak hodnota presahuje celkovú veľkosť dokumentov, ktoré je možné načítať (predvolená hodnota je 10,240 MB), kontaktujte technickú podporu.

3. Počkajte asi 15 minút a skontrolujte, či máte prístup k online pomoci zariadenia smerujúceho na juh, ku ktorému nie je možné získať prístup z dôvodu preťaženej veľkosti dokumentu.
- Ak áno, manuálne zrušte alarm.
 - Ak nie, kontaktujte technickú podporu.

Vymazanie alarmu

ADMC: Po odstránení poruchy musíte tento alarm manuálne vymazať.

ALM-100003 Platnosť certifikátu čoskoro vyprší

Popis alarmu

- Správa certifikátov kontroluje platnosť certifikátu v určenom intervale (štandardne každý deň alebo každých 24 hodín podľa časovej jednotky). Keď je aktivované hlásenie alarmu certifikátu, tento alarm sa generuje, keď správa certifikátu zistí, že zostávajúca doba platnosti certifikátu identity alebo dôveryhodného certifikátu v správe certifikátov je rovnaká alebo menšia ako prah generovania alarmu (v predvolenom nastavení 90 dní alebo 2160 hodín podľa časová jednotka).
- Správa certifikátov kontroluje platnosť zoznamov zrušených certifikátov (CRL) v určených intervaloch (štandardne každý deň alebo každých 24 hodín podľa časovej jednotky). Keď je povolené hlásenie alarmu certifikátu, tento alarm sa generuje, keď správa certifikátov zistí, že zostávajúca doba platnosti CRL v správe certifikátov je menšia alebo rovná 5 % časového rozdielu medzi **Next Update Time** a **Issued By**.

NOTE

Kontrolný interval a prah generovania alarmu môžete nakonfigurovať v časti **Certificate Alarm Configurations**.

1. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
2. Na navigačnej table vyberte **Settings > General Configurations**.
3. V oblasti **Certificate Alarm Configurations** kliknite na položku **Modify**.
4. Zapnite **Certificate alarm**. Nastavte **Time unit**, **Check interval** a **In advance alarm before certificate expires**.
5. Kliknite na tlačidlo **Save**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
100003	Menší	Alarm v časovej doméne

Parametre alarmu

Katégoria	Parameter	Popis
Informácie o polohe	Názov služby	Názov služby, ktorej certifikát patrí.
	Typ služby	Typ služby, ku ktorej certifikát patrí. Napríklad: International
	Typ certifikátu	Typ certifikátu. Hodnota môže byť:

Kategória	Parameter	Popis
		<ul style="list-style-type: none"> • Certifikát dôveryhodnosti • Osvedčenie totožnosti • Zrušený certifikát
	Vydal	Vydavateľ identity alebo dôveryhodného certifikátu alebo CRL.
	Vydané pre	Používateľ identity alebo dôveryhodného certifikátu.
	Platný do	Čas, kedy vyprší platnosť certifikátu identity alebo dôveryhodnosti.
	Ďalší čas aktualizácie	Čas vypršania platnosti CRL.
Ďalšie informácie	Vydal	Vydavateľ identity alebo dôveryhodného certifikátu alebo CRL.
	Vydané pre	Používateľ identity alebo dôveryhodného certifikátu.

Vplyv na systém

Služba, ktorej certifikát patrí, sa môže stať abnormálnou.

Možné príčiny

Doba platnosti certifikátu je kratšia ako 30 dní.

Postup

1. V oblasti **Location Info** na karte **Details** alarmu skontrolujte a zaznamenajte informácie o certifikáte, ktorého platnosť čoskoro vyprší.
 - a. Vyberte si z hlavného menu.
 - b. Kliknite na položku **Certificate Is About to Expire**.
 - c. V oblasti **Location Info** si zaznamenajte hodnoty nasledujúcich parametrov:
 - Názov služby
 - Typ certifikátu
 - Vydal
 - Vydané pre
 - Platný do
 - Ďalší čas aktualizácie

2. Vykonaťte operácie na základe tabuľky 1.

Tabuľka 1 Metódy odstraňovania problémov pre rôzne certifikáty


Názov služby	Typ certifikátu	Metóda
Názov služby v správe certifikátov služieb .	Osvedčenie totožnosti	Prejdite na 3.
	Certifikát dôveryhodnosti	Prejdite na 4.
	Zrušený certifikát	Prejdite na 5.
Zdieľané zoznamy CRL	Zrušený certifikát	Prejdite na 6.

3. Aktualizujte certifikát totožnosti.

- a. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
- b. Kliknite na kartu zodpovedajúcu hodnote **Service Name** zaznamenananej v 1.c.
- c. V zozname certifikátov totožnosti vyhľadajte zodpovedajúci certifikát na základe hodnôt **Issued By, Issued To** a **Valid To** zaznamenaných v 1.c.
- d. Ak chcete získať nový súbor verejného kľúča, súbor súkromných kľúčov alebo reťaz certifikátov a heslo pre súkromný kľúč, kontaktujte správcu systému.
- e. Kliknite na položku **Import**.
- f. Podľa výzvy nakonfigurujte informácie o certifikáte.
- g. Kliknite na tlačidlo **Submit**.
- h. V dialógovom okne **High Risk** si pozorne prečítajte informácie a potvrdte, či chcete aktualizovať certifikát.
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 3.i.
 - Ak nie, kliknite na tlačidlo **Cancel**.
- i. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
- j. (Voliteľné) Na základe informácií zobrazených na stránke určite, či sú na dokončenie aktualizácie certifikátu potrebné ďalšie operácie, ako napríklad reštartovanie služby.
 - Ak áno, vykonajte ďalšie operácie na základe zobrazených informácií.
 - Ak nie, aktualizácia certifikátu je dokončená.


4. Aktualizujte certifikát dôveryhodnosti.


- a. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
- b. Kliknite na kartu zodpovedajúcu hodnote **Service Name** zaznamenananej v 1.c.

- c. V zozname dôveryhodných certifikátov vyhľadajte zodpovedajúci certifikát na základe hodnôt **Issued By**, **Issued To** a **Valid To** zaznamenaných v 1.c.
- d. Kliknite  na stĺpec **Operation** v riadku, ktorý obsahuje certifikát.
- e. V dialógovom okne **High Risk** si pozorne prečítajte informácie a potvrdte, či chcete aktualizovať certifikát.
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na tlačidlo **OK** a prejdite na 4.f.
 - Ak nie, kliknite na tlačidlo **Cancel**.
- f. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
- g. Ak chcete získať nový súbor certifikátu, kontaktujte správcu systému.

NOTE

Ak je nový certifikát vo formáte PKCS12 alebo JKS, získajte heslo pre certifikát.

- h. Kliknite na položku **Import**.
 - i. Podľa výzvy nakonfigurujte informácie o certifikáte.
 - j. Kliknite na tlačidlo **Submit**.
 - k. (Voliteľné) Pozorne si prečítajte informácie a potvrdte, či chcete odovzdať súbor certifikátu v dialógovom okne **Rsk**, ak súbor certifikátu, ktorý sa má odovzdať, obsahuje nezabezpečené informácie (napríklad sa používa nezabezpečený algoritmus).
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 4.l.
 - Ak nie, kliknite na tlačidlo **Cancel**.
 - l. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
 - m. (Voliteľné) Na základe informácií zobrazených na stránke určite, či sú na dokončenie aktualizácie certifikátu potrebné ďalšie operácie, ako napríklad reštartovanie služby.
 - Ak áno, vykonajte ďalšie operácie na základe zobrazených informácií.
 - Ak nie, aktualizácia certifikátu je dokončená.
5. Aktualizujte zoznam CRL používaný každou službou.
- a. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
 - b. Kliknite na kartu zodpovedajúcu hodnote **Service Name** zaznamenananej v 1.c.
 - c. V zozname CRL vyhľadajte zodpovedajúce CRL na základe hodnôt **Issued By** a **Next Update Time** zaznamenaných v 1.c.
 - d. Kliknite  do stĺpca **Operation** v riadku, ktorý obsahuje CRL.

- e. V dialógovom okne **High Risk** si pozorne prečítajte informácie a potvrdte, či chcete aktualizovať CRL.
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na tlačidlo **OK** a prejdite na 5.f.
 - Ak nie, kliknite na tlačidlo **Cancel**.
 - f. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
 - g. Ak chcete získať nové CRL, kontaktujte správcu systému.
 - h. Kliknite na položku **Import**.
 - i. Podľa výzvy nakonfigurujte informácie CRL.
 - j. Kliknite na tlačidlo **Submit**.
 - k. (Voliteľné) Pozorne si prečítajte informácie a potvrdte, či chcete odovzdať súbor CRL v dialógovom okne **Risk**, ak súbor CRL, ktorý sa má odovzdať, obsahuje nezabezpečené informácie (napríklad sa používa nezabezpečený algoritmus).
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 5.l.
 - Ak nie, kliknite na tlačidlo **Cancel**.
 - l. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
 - m. (Voliteľné) Na základe informácií zobrazených na stránke určite, či sú na dokončenie aktualizácie CRL potrebné ďalšie operácie, ako napríklad reštartovanie služby.
 - Ak áno, vykonajte ďalšie operácie na základe zobrazených informácií.
 - Ak nie, aktualizácia CRL je dokončená.
6. Aktualizujte zoznamy CRL v zozname zdieľaných zoznamov CRL.
- a. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
 - b. Na navigačnej table vyberte **Shared CRLs**.
 - c. V zozname CRL vyhľadajte zodpovedajúce CRL na základe hodnôt **Issued By** a **Next Update Time** zaznamenaných v 1.c.
 - d. Kliknite  do stĺpca **Operation** v riadku, ktorý obsahuje CRL.
 - e. V dialógovom okne **High Risk** si pozorne prečítajte informácie a potvrdte, či chcete aktualizovať CRL.
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 6.f.
 - Ak nie, kliknite na tlačidlo **Cancel**.
 - f. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.

- g. Ak chcete získať nové CRL, kontaktujte správcu systému.
- h. Kliknite na položku **Import**.
- i. Podľa výzvy nakonfigurujte informácie CRL.
- j. Kliknite na tlačidlo **Submit**.
- k. (Voliteľné) Pozorne si prečítajte informácie a potvrdte, či chcete odovzdať súbor CRL v dialógovom okne **Risk** , ak súbor CRL, ktorý sa má odovzdať, obsahuje nezabezpečené informácie (napríklad sa používa nezabezpečený algoritmus).
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 6.l.
 - Ak nie, kliknite na tlačidlo **Cancel**.
- l. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK** .

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-100005 Platnosť certifikátu vypršala

Popis alarmu

Správa certifikátov kontroluje platnosť certifikátu v určenom intervale (štandardne každý deň alebo každých 24 hodín podľa časovej jednotky). Keď je povolené hlásenie alarmu certifikátu, tento alarm sa generuje, keď správa certifikátov zistí, že platnosť certifikátu v správe certifikátov vypršala.

NOTE

Interval kontroly môžete nakonfigurovať takto:

1. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
2. Na navigačnej table vyberte **Settings > General Configurations**.
3. V oblasti **Certificate Alarm Configurations** kliknite na položku **Modify**.
4. Zapnite **Certificate alarm**. Nastavte **Time unit**, **Check interval** a **In advance alarm before certificate expires**.
5. Kliknite na tlačidlo **Save**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
100005	Major	Alarm v časovej doméne

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Názov služby	Názov služby, ktorej certifikát patrí.
	Typ služby	Typ služby, ku ktorej certifikát patrí. Napríklad: International
	Typ certifikátu	Typ certifikátu. Hodnota môže byť: <ul style="list-style-type: none">• Certifikát dôveryhodnosti• Osvedčenie totožnosti• Zrušený certifikát
	Vydal	Vydavateľ identity alebo dôveryhodného certifikátu alebo CRL.
	Vydané pre	Používateľ identity alebo dôveryhodného certifikátu.
	Platný do	Čas, kedy vyprší platnosť certifikátu identity alebo dôveryhodnosti.

Kategória	Parameter	Popis
	Ďalší čas aktualizácie	Čas vypršania platnosti CRL.
Ďalšie informácie	Vydal	Vydavateľ identity alebo dôveryhodného certifikátu alebo CRL.
	Vydané pre	Používateľ identity alebo dôveryhodného certifikátu.

Vplyv na systém

Služba, ktorej certifikát patrí, sa stáva abnormálnou.

Možné príčiny

Platnosť certifikátu vypršala.

Postup

1. V oblasti **Location Info** na karte **Details** alarmu skontrolujte a zaznamenajte informácie o certifikáte, ktorého platnosť vypršala.
 - a. Vyberte si z hlavného menu.
 - b. Kliknite na položku **Certificate Has Expired**.
 - c. V oblasti **Location Info** si zaznamenajte hodnoty nasledujúcich parametrov:
 - Názov služby
 - Typ certifikátu
 - Vydal
 - Vydané pre
 - Platný do
2. Vykonajte operácie na základe tabuľky 1.


Tabuľka 1 Metódy odstraňovania problémov pre rôzne certifikáty

Názov služby	Typ certifikátu	Metóda
Názov služby v správe certifikátov služieb .	Osvedčenie totožnosti	Prejdite na 3.
	Certifikát dôveryhodnosti	Prejdite na 4.
	Zrušený certifikát	Prejdite na 5.
Zdieľané zoznamy CRL	Zrušený certifikát	Prejdite na 6.

3. Aktualizujte certifikát totožnosti.


- a. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
- b. Kliknite na kartu zodpovedajúcu hodnote **Service Name** zaznamenananej v 1.c.
- c. V zozname certifikátov totožnosti vyhľadajte zodpovedajúci certifikát na základe hodnôt **Issued By, Issued To** a **Valid To** zaznamenaných v 1.c.
- d. Ak chcete získať nový súbor verejného kľúča, súbor súkromných kľúčov alebo reťaz certifikátov a heslo pre súkromný kľúč, kontaktujte správcu systému.
- e. Kliknite na položku **Import**.
- f. Podľa výzvy nakonfigurujte informácie o certifikáte.
- g. Kliknite na tlačidlo **Submit**.
- h. V dialógovom okne **High Risk** si pozorne prečítajte informácie a potvrdte, či chcete aktualizovať certifikát.
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 3.i.
 - Ak nie, kliknite na tlačidlo **Cancel**.
- i. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
- j. (Voliteľné) Na základe informácií zobrazených na stránke určite, či sú na dokončenie aktualizácie certifikátu potrebné ďalšie operácie, ako napríklad reštartovanie služby.
 - Ak áno, vykonajte ďalšie operácie na základe zobrazených informácií.
 - Ak nie, aktualizácia certifikátu je dokončená.


4. Aktualizujte certifikát dôveryhodnosti.

- a. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
- b. Kliknite na kartu zodpovedajúcu hodnote **Service Name** zaznamenananej v 1.c.
- c. V zozname dôveryhodných certifikátov vyhľadajte zodpovedajúci certifikát na základe hodnôt **Issued By, Issued To**, a **Valid To** zaznamenaných v 1.c.
- d. Kliknite  na riadok, ktorý obsahuje certifikát.
- e. V dialógovom okne **High Risk** si pozorne prečítajte informácie a potvrdte, či chcete aktualizovať certifikát.
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na tlačidlo **OK** a prejdite na 4.f.
 - Ak nie, kliknite na tlačidlo **Cancel**.
- f. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
- g. Ak chcete získať nový súbor certifikátu, kontaktujte správcu systému.

NOTE

Ak je nový certifikát vo formáte PKCS12 alebo JKS, získajte heslo pre certifikát.

- h. Kliknite na položku **Import**.
 - i. Podľa výzvy nakonfigurujte informácie o certifikáte.
 - j. Kliknite na tlačidlo **Submit**.
 - k. (Voliteľné) Pozorne si prečítajte informácie a potvrdte, či chcete odovzdať súbor certifikátu v dialógovom okne **Risk**, ak súbor certifikátu, ktorý sa má odovzdať, obsahuje nezabezpečené informácie (napríklad sa používa nezabezpečený algoritmus).
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 4.l.
 - Ak nie, kliknite na tlačidlo **Cancel**.
 - l. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
 - m. (Voliteľné) Na základe informácií zobrazených na stránke určite, či sú na dokončenie aktualizácie certifikátu potrebné ďalšie operácie, ako napríklad reštartovanie služby.
 - Ak áno, vykonajte ďalšie operácie na základe zobrazených informácií.
 - Ak nie, aktualizácia certifikátu je dokončená.
5. Aktualizujte zoznam CRL používaný každou službou.
- a. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
 - b. Kliknite na kartu zodpovedajúcu hodnote **Service Name** zaznamenananej v 1.c.
 - c. V zozname CRL vyhľadajte zodpovedajúce CRL na základe hodnôt **Issued By** a **Next Update Time** zaznamenaných v 1.c.
 - d. Kliknite  do stĺpca **Operation** v riadku, ktorý obsahuje CRL.
 - e. V dialógovom okne **High Risk** si pozorne prečítajte informácie a potvrdte, či chcete aktualizovať CRL.
 - Ak áno, vyberte **I understand the risk and want to continue**, kliknite na tlačidlo **OK** a prejdite na 5.f.
 - Ak nie, kliknite na tlačidlo **Cancel**.
 - f. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
 - g. Ak chcete získať nové CRL, kontaktujte správcu systému.
 - h. Kliknite na položku **Import**.
 - i. Podľa výzvy nakonfigurujte informácie CRL.
 - j. Kliknite na tlačidlo **Submit**.
 - k. (Voliteľné) Pozorne si prečítajte informácie a potvrdte, či chcete odovzdať súbor CRL v dialógovom okne **Risk**, ak súbor CRL, ktorý sa má odovzdať, obsahuje nezabezpečené informácie (napríklad sa používa nezabezpečený algoritmus).

- Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 5.l.
 - Ak nie, kliknite na tlačidlo **Cancel**.
- l. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
- m. (Voliteľné) Na základe informácií zobrazených na stránke určite, či sú na dokončenie aktualizácie CRL potrebné ďalšie operácie, ako napríklad reštartovanie služby.
- Ak áno, vykonajte ďalšie operácie na základe zobrazených informácií.
 - Ak nie, aktualizácia CRL je dokončená.
6. Aktualizujte zoznamy CRL v zozname zdieľaných zoznamov CRL.
- a. Z hlavnej ponuky vyberte **System > About > Certificate Management**.
- b. Na navigačnej table vyberte **Shared CRLs**.
- c. V zozname CRL vyhľadajte zodpovedajúce CRL na základe hodnôt **Issued By** a **Next Update Time** zaznamenaných v 1.c.
- d. Kliknite  do stĺpca **Operation** v riadku, ktorý obsahuje CRL.
- e. V dialógovom okne **High Risk** si pozorne prečítajte informácie a potvrdte, či chcete aktualizovať CRL.
- Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 6.f.
 - Ak nie, kliknite na tlačidlo **Cancel**.
- f. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.
- g. Ak chcete získať nové CRL, kontaktujte správcu systému.
- h. Kliknite na položku **Import**.
- i. Podľa výzvy nakonfigurujte informácie CRL.
- j. Kliknite na tlačidlo **Submit**.
- k. (Voliteľné) Pozorne si prečítajte informácie a potvrdte, či chcete odovzdať súbor CRL v dialógovom okne **Risk**, ak súbor CRL, ktorý sa má odovzdať, obsahuje nezabezpečené informácie (napríklad sa používa nezabezpečený algoritmus).
- Ak áno, vyberte **I understand the risk and want to continue**, kliknite na **OK** a prejdite na 6.l.
 - Ak nie, kliknite na tlačidlo **Cancel**.
- l. V dialógovom okne **Information** si pozorne prečítajte informácie a kliknite na tlačidlo **OK**.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-100006 Zlyhania autentifikácie dosahujú maximum

Popis alarmu

Po prepojení systému tretej strany so SmartPVMS prostredníctvom NBI, SmartPVMS overí systém tretej strany. Štandardne sa tento alarm generuje, keď overenie zlyhá trikrát za sebou počas 60 minút a IP adresa systému tretej strany je zablokovaná.

NOTE

Maximálny počet po sebe nasledujúcich zlyhaní autentifikácie, ktoré spustia generovanie alarmu, a dobu blokovania je možné nakonfigurovať v **Security Settings**.

1. Z hlavnej ponuky vyberte **System > System Settings > Northbound Interface**.
2. Na navigačnej table vyberte **SNMP NBI > Security Settings**.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
100006	Kritické	Bezpečnostný alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	IP adresa	IP adresa systému tretej strany.
Ďalšie informácie	Maximálny počet pokusov o prihlásenie	Tento alarm sa generuje, keď počet po sebe idúcich zlyhaní autentifikácie systému tretej strany v určenom období dosiahne maximum. Napríklad, ak je Login period nastavená na 60 minút a Maximum number of login attempts je nastavený na 3 , tento alarm sa vygeneruje, keď overenie zlyhá trikrát za sebou v priebehu 60 minút.

Vplyv na systém

Systém tretej strany sa nedokáže prepojiť so SmartPVMS cez NBI a alarmy zhromaždené systémom SmartPVMS nemožno nahlásiť do systému tretej strany.

Možné príčiny

Overovacie informácie o SmartPVMS nakonfigurovaný v systéme tretej strany je nesprávny.

Postup

1. Z hlavnej ponuky vyberte **System > System Settings > Northbound Interface**.
2. Na navigačnej table vyberte **SNMP NBI > Third-party System Settings**.
3. V zozname nastavení systému tretej strany kliknite na ikonu **Edit** v stĺpci **Operation** v riadku, ktorý obsahuje požadovanú IP adresu.
4. Poradte sa so správcom systému tretej strany, aby ste zistili nastavenia parametrov na tejto stránke, ktoré nie sú konzistentné so systémom tretej strany, zmeňte nekonzistentné nastavenia tak, aby boli konzistentné so systémom tretej strany, a kliknite na tlačidlo **Save**.

Vymazanie alarmu

ADAC: Po vygenerovaní alarmu je IP adresa systému tretej strany zablokovaná. Po uplynutí doby uzamknutia nakonfigurovanej v **Security Settings** sa adresa IP automaticky odomkne. Po odomknutí IP adresy sa alarm automaticky vymaže. Manuálne čistenie nie je potrebné.

ALM-100007 Abnormálna kontrola stavu poplachovej služby

Popis alarmu

Tento alarm sa generuje, keď systém zistí výnimku počas úplného spracovania aktuálnej vyrovnávacej pamäte alarmov, výpisu alarmov alebo delenia tabuľky (Keď počet alarmov v tabuľke historických alarmov dosiahne hornú hranicu, systém automaticky vytvorí tabuľku na uloženie nasledujúcich alarmov. údaje.).

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
100007	Major	Alarm kvality služby

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Typ výnimky	Typ abnormálnej úlohy, ktorá spôsobuje tento alarm. <ul style="list-style-type: none">Úplná výnimka spracovania aktuálnej pamäte cache alebo výnimka úlohy rozdelenia tabuľkyVýnimka úlohy výpisu Tento parameter sa zobrazuje v časti Location Info .
	Alarmy maximálneho prúdu	Maximálny počet aktuálnych alarmov v databáze. Tento parameter sa zobrazuje v Location Info iba vtedy, keď je hodnota Exception type is Full current alarm cache processing exception or table division task exception .
	Alarmy abnormálneho maximálneho prúdu	Tento parameter sa zobrazí iba vtedy, keď hodnota Maximum current alarms nie je v rozsahu hodnôt nastavenom v systéme. Tento parameter sa zobrazuje v Location Info iba vtedy, keď je hodnota Exception type is Full current alarm cache processing exception or table division task exception . Zobrazuje sa len jeden z Maximum current alarms a Abnormal maximum current alarms .
	Celkový počet aktuálnych alarmov	Celkový počet aktuálnych alarmov v databáze. Tento parameter sa zobrazuje v Location Info iba vtedy, keď je hodnota Exception type is Full current alarm cache processing exception or table division task exception .

Kategória	Parameter	Popis
	Nehistorické alarmy	Celkový počet nehistorických alarmov v databáze. Tento parameter sa zobrazuje v Location Info iba vtedy, keď je hodnota Exception type is Full current alarm cache processing exception or table division task exception .
	Historické alarmy	Celkový počet historických alarmov v databáze. Tento parameter sa zobrazuje v Location Info iba vtedy, keď je hodnota Exception type is Full current alarm cache processing exception or table division task exception .
	Celková kapacita databázy	Celková kapacita databázy alarmov. Tento parameter sa zobrazuje v Location Info len vtedy, keď je hodnota Exception type is Dump task exception .
	Využitá kapacita databázy	Využitá kapacita databázy alarmov. Tento parameter sa zobrazuje v Location Info len vtedy, keď je hodnota Exception type is Dump task exception .
	Využitie databázy	Pomer využitej kapacity databázy k celkovej kapacite databázy. Tento parameter sa zobrazuje v Location Info len vtedy, keď je hodnota Exception type is Dump task exception .

Vplyv na systém

- Po dosiahnutí maximálneho počtu alarmov na stránke **Current Alarms** sa nové hlásené alarmy nezobrazia na stránke **Current Alarms**.
- Keď vykonávate operácie na stránke alarmu, zobrazí sa správa, ktorá indikuje, že systém je zaneprázdnený alebo abnormálny.

Možné príčiny

- Databáza je abnormálna.
- Počas delenia tabuľky sa vyskytne výnimka alebo sa vyskytne chyba počas aktualizácie informácií tabuľky údajov.
- Miesto na disku v uzle je nedostatočné.
- Povolenie na zápis pre adresár výpisu je abnormálne.

Postup

Získajte **Location Info** alarmu a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-100450 Zistila sa nezákonná požiadavka

Popis alarmu

Tento alarm sa generuje, keď APIManager prijme žiadosti o prístup odoslané zo severných API a počet po sebe nasledujúcich zlyhaní autentifikácie prekročí horný limit (štandardne päťkrát).

NOTE

Podrobnosti o konfigurácii maximálneho počtu pokusov o autentifikáciu nájdete v "serviceConfig.sh" v *Command Reference*.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
100450	Menší	Bezpečnostný alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Názov služby	Názov služby, ktorá hlási alarm.
	IP adresa servera	IP adresa servera, ktorý hlási alarm.
	IP adresa klienta	IP adresa klienta, ktorý hlási alarm.


Vplyv na systém

APIManager môže byť napadnutý neoprávnenými požiadavkami, čo ovplyvňuje výkon služby.

Možné príčiny

- Používateľ prepojenia nemá povolenie na prístup k severným rozhraniam API.
- Platnosť tokenu používateľa prepojenia vypršala.
- Používateľské meno alebo heslo používateľa prepojenia je nesprávne.
- IP adresa klienta požiadavky nie je autorizovanou IP adresou.

Postup

1. Vyberte si z hlavného menu.
2. Kliknite  na riadok, ktorý obsahuje alarm **Illegal request detected**. Na karte **Details** zobrazte **Local Info** a **Possible Causes**.
3. Vykonajte zodpovedajúcu operáciu podľa možnej príčiny alarmu.

Možné príčiny	Spôsob prevádzky
Používateľ prepojenia nemá povolenie na prístup k severným rozhraniam API.	<p>Udeľte používateľovi povolenia na prístup k severným rozhraniam API.</p> <p>Obráťte sa na správcu zabezpečenia, aby používateľovi udelil povolenia rozhrania API smerujúce na sever.</p> <ol style="list-style-type: none">1. Z hlavnej ponuky vyberte System > System Management > User Management.2. Na ľavej navigačnej table vyberte položku Roles.3. Na stránke Roles kliknite na položku Create.4. Na zobrazenej stránke nastavte základné informácie o úlohe.5. Vyberte používateľov, ktorí majú byť priradení k role, a kliknite na tlačidlo Next. <p>Po dokončení autorizácie roly budú mať používatelia, ktorých ste vybrali, povolenia zahrnuté do tejto roly.</p> <ol style="list-style-type: none">6. Kliknite na tlačidlo Next.7. Kliknite na Application-Level Operation Rights na karte Select Operation Rights, aby ste nastavili operačné práva roly na úrovni aplikácie.8. Vyberte API Management, kliknite na OK.
Platnosť tokenu používateľa prepojenia vypršala.	<p>Klient potrebuje token znova získať na aktualizáciu. Kontaktujte technickú podporu.</p>
Používateľské meno alebo heslo používateľa prepojenia je nesprávne.	<p>Získajte platné používateľské meno a heslo.</p> <p>Ak chcete získať platné používateľské meno a heslo na prístup k severnému API, kontaktujte správcu.</p>
IP adresa klienta požiadavky nie je autorizovanou IP adresou.	<p>Udeľte povolenie na prístup k IP adrese.</p> <p>Obráťte sa na bezpečnostného správcu, aby používateľovi udelil povolenia na prístup k IP adrese.</p>

Možné príčiny	Spôsob prevádzky
	<p>9. Z hlavnej ponuky vyberte System > System Management > User Policies.</p> <p>10. Na navigačnom paneli vyberte položku Client IP Address Policies.</p> <p>11. Na stránke Client IP Address Policies kliknite na položku Create.</p> <p>12. Nastavte politiku IP adresy klienta a kliknite na OK.</p> <p>Nová politika adresy IP klienta nadobudne účinnosť až po jej aplikovaní na používateľa.</p> <p>13. Z hlavnej ponuky vyberte System > System Management > User Management.</p> <p>14. Na navigačnej table vyberte položku Users. Na stránke Users kliknite na používateľské meno.</p> <p>15. Na karte Access Policies na položku Create.</p> <p>16. Vyberte požadované zásady adresy IP klienta a kliknite na tlačidlo OK.</p>
Iné príčiny	Kontaktujte technickú podporu.

Vymazanie alarmu

ADMC: Po odstránení poruchy musíte tento alarm manuálne vymazať.

ALM-100503 Test pripojenia oblasti nasadenia zlyhal

Popis alarmu

Tento alarm sa generuje, keď je sieť v regióne odpojená.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
100503	Major	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	servis	Názov služby, ktorá hlási alarmy.
	Názov regiónu	Názov oblasti, ktorá neprešla testom pripojenia.
	ID regiónu	ID oblasti, ktorá neprešla testom pripojenia.
	Adresa IP regiónu	IP adresa regiónu, ktorý neprešiel testom pripojenia.

Vplyv na systém

Všetky funkcie v regióne sú nedostupné.

Možné príčiny

- Regionálna sieť je odpojená.
- Región má chybné služby, napríklad chybné regionálne služby, chybné regionálne autobusové služby alebo chybné služby prístupu k regiónu.

Postup

1. Obráťte sa na správcu siete a overte si pripojenie k regionálnej sieti.
 - Ak je pripojenie abnormálne, kontaktujte technickú podporu.
 - Ak je pripojenie normálne, prejdite na 2.
2. Obráťte sa na technickú podporu, aby ste skontrolovali denník DriverMgmtService a na základe informácií z denníka odstránili poruchu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-101200 Abnormálna replikácia

Popis alarmu

Tento alarm sa generuje, keď systém DR detekuje (detekcia sa vykonáva každých 30 sekúnd) jednu z nasledujúcich udalostí v troch po sebe nasledujúcich časoch: sieť medzi aktívnym miestom a pohotovostným miestom je oneskorená, synchronizácia údajov medzi aktívnym miestom a pohotovostným miestom je abnormálna alebo sa synchronizácia údajov oneskorí z dôvodu veľkého objemu údajov. Tento alarm sa automaticky vymaže, keď je sieť normálna alebo keď je normálna alebo dokončená synchronizácia údajov.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101200	Kritické	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Alias produktu 1	Produktový alias stránky.
	Alias produktu 2	Produktový alias stránky.
	názov	Názov inštancie databázy.
	Typ	Typ inštancie.

Vplyv na systém

- Údaje nemožno replikovať medzi aktívnou lokalitou a produktmi pohotovostnej lokality.
- Nie je možné vykonať prepnutie medzi produktmi aktívnej lokality a pohotovostným režimom lokality.
- Po násilnom prevzatí služby produktu aktívnej lokality produktom pohotovostnej lokality sa niektoré údaje produktu pohotovostnej lokality stratia.

Možné príčiny

- O produkte existuje veľké množstvo údajov.
- Nepodarilo sa synchronizovať používateľské údaje medzi aktívnou lokalitou a pohotovostnou lokalitou.
- Stav srdcového tepu medzi aktívnym miestom a miestom pohotovostného režimu je abnormálny.
- Sieť na replikáciu údajov medzi aktívnou lokalitou a pohotovostnou lokalitou je abnormálna.
- Služba replikácie údajov je abnormálna.

- Stav lokálnej replikácie inštancií hlavnej alebo podriadenej databázy je abnormálny.

Postup

1. Poruchu odstráňte podľa nasledujúcej tabuľky.

NOTE

Táto časť poskytuje iba základné metódy riešenia problémov. Ak porucha pretrváva aj po odstránení problémov pomocou tejto metódy, kontaktujte technickú podporu.

Tabuľka 1 Skontrolujte položky

Skontrolujte položku	Skontrolujte metódu	Riešenie
Skontrolujte, či sieť systému DR nie je chybná.	<p>Nasledujúci text popisuje, ako skontrolovať pripojenie srdcového tepu medzi aktívnou lokalitou a pohotovostnou lokalitou:</p> <ol style="list-style-type: none"> 1. Použite PuTTY na prihlásenie do riadiaceho uzla na aktívnom mieste ako používateľ sopuser v režime SSH. <p>POZNÁMKA:</p> <p>Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 alebo Management1 . Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Querying the Management IP Address of a Node“ v <i>Administrator Guide</i>.</p> <ol style="list-style-type: none"> 2. Spustíte nasledujúci príkaz na otestovanie konektivity medzi riadiacimi uzlami na aktívnej lokalite a lokalite v pohotovostnom režime: <ul style="list-style-type: none"> • Pre adresu IPv4 spustíte nasledujúci príkaz: > ping <i>IP address of the management node at the standby site</i> • Pre adresu IPv6 spustíte nasledujúci príkaz: > ping6 <i>IP address of the</i> 	Kontaktujte správcu, aby skontroloval stav siete a odstránil poruchu siete.

Tabuľka 1 Skontrolujte položky

Skontrolujte položku	Skontrolujte metódu	Riešenie
	<p><i>management node at the standby site</i>Skontrolujte výstup príkazu.</p> <ul style="list-style-type: none"> • Ak sa zobrazia informácie podobné nasledujúcim, IP adresa môže byť testovaná a sieťové pripojenie je normálne: <pre>64 bytes from IP address of the management node at the standby site: icmp_seq=1 ttl=251 time=42.1 ms</pre> <ul style="list-style-type: none"> • Ak sa do 1 minúty nezobrazí žiadny príkaz, je sieťové pripojenie abnormálne. <p>3. Stlačením Ctrl+C zastavíte príkaz ping.</p>	
<p>Skontrolujte, či je srdcový tep systému DR normálny.</p>	<p>Skontrolujte, či sa negeneruje alarm „ALM-101201 Abnormal Heartbeat“.</p>	<p>Podrobnosti nájdete v časti ALM-101201 Abnormal Heartbeat .</p>
<p>Skontrolujte, či má <i>inštalčný adresár /tmp /manager</i> oprávnenie na zápis.</p>	<ol style="list-style-type: none"> 1. Použite PuTTY na prihlásenie do riadiaceho uzla v pohotovostnom režime ako používateľ sopuser v režime SSH. <p>POZNÁMKA:</p> <p>Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 a potom na Management1. Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Querying the Management IP Address of a Node“ v <i>Administrator Guide</i>.</p> <ol style="list-style-type: none"> 2. Ak chcete prepnúť na používateľa ossadm, spustíte nasledujúci príkaz: > su - ossadm <pre>Password: password for the ossadm user</pre> <ol style="list-style-type: none"> 3. Spustíte nasledujúce príkazy, aby ste skontrolovali povolenia v <i>inštalčnom adresári /tmp /manager</i>: 	<ol style="list-style-type: none"> 1. Použite PuTTY na prihlásenie do riadiaceho uzla v pohotovostnom režime ako používateľ sopuser v režime SSH. <p>POZNÁMKA:</p> <p>Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 a potom na Management1 . Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Querying the Management IP Address of a Node“ v <i>Administrator Guide</i>.</p> <ol style="list-style-type: none"> 2. Ak chcete prepnúť na používateľa ossadm, spustíte nasledujúci príkaz: > su - ossadm <pre>Password: password for the ossadm user</pre>

Tabuľka 1 Skontrolujte položky

Skontrolujte položku	Skontrolujte metódu	Riešenie
	<p>> <i>inštalačný adresár</i> cd /tmp > ll Zobrazia sa informácie podobné nasledujúcim. Skontrolujte, či je povolenie v adresári manager drwxr-x-- - .</p> <pre data-bbox="541 602 1074 786">total 40 ... drwxr-x---. 29 *** ossgroup 4096 Mar 6 15:39 manager ...</pre> <ul style="list-style-type: none"> • Ak áno, skontrolujte ďalšie poruchy. • Ak nie, nastavte povolenie pre adresár. 	<p>3. Spustíte nasledujúci príkaz na nastavenie povolení pre <i>inštalačný adresár</i> /tmp /manager: > <i>inštalačný adresár</i> chown -R 750 /tmp /manager</p>
<p>Skontrolujte inštancie databázy.</p>	<ol style="list-style-type: none"> 1. Prihláste sa do PowerEcho aktívnej lokality a pohotovostnej lokality. <ol style="list-style-type: none"> a. Prístup k PowerEcho získate na https://client IP address of the PowerEcho:31945. <div data-bbox="541 1198 1062 1408" style="background-color: #ffffcc; padding: 5px;"> <p>POZNÁMKA: Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.</p> </div> <ol style="list-style-type: none"> b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo Log In . 2. Na PowerEcho vyberte z hlavnej ponuky HA > Remote High Availability System > Manage DR System. 3. Skontrolujte, či je stav synchronizácie údajov Abnormal. <ul style="list-style-type: none"> • Ak áno, synchronizácia údajov je abnormálna. Vykonajte 4 a skontrolujte typ údajov. 	<p>Podrobnosti nájdete v časti „Database Faults“ v <i>príručke Troubleshooting Guide</i>.</p>


Tabuľka 1 Skontrolujte položky

Skontrolujte položku	Skontrolujte metódu	Riešenie
	<ul style="list-style-type: none"> • Ak nie, synchronizácia údajov je normálna. Skontrolujte ďalšie poruchy. <ol style="list-style-type: none"> 4. Kliknutím > rozbalíte podrobnosti o synchronizácii údajov o produkte. 5. Zaznamenajte typy údajov produktu, ktorého Status je Abnormal . 	
<p>Skontrolujte lokálne hlavné a podriadené inštancie databázy.</p>	<ol style="list-style-type: none"> 1. Prihláste sa do PowerEcho aktívnej lokality a pohotovostnej lokality. <ol style="list-style-type: none"> a. Prístup k PowerEcho získate na https://client IP address of the PowerEcho:31945. <div style="background-color: #ffffcc; padding: 5px; margin: 5px 0;"> <p>POZNÁMKA: Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.</p> </div> <ol style="list-style-type: none"> b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo Log In. 2. Z hlavnej ponuky vyberte Maintenance > Operation and Maintenance Management > Panoramic Monitoring. 3. Na navigačnej table vyberte položku Middleware Monitoring. 4. V ľavom hornom rohu stránky Middleware Monitoring vyberte produkt. 5. Na záložke Relational Databases skontrolujte, či sú inštancie hlavnej a podriadenej databázy normálne. Ak sú hodnoty Status inštancií hlavnej a podriadenej databázy Running a hodnoty Replication Status sú Normal, inštancie databázy sú normálne. V opačnom prípade poruchu odstráňte. 	<p>Podrobnosti nájdete v časti „Database Faults“ v príručke <i>Troubleshooting Guide</i>.</p>

2. Nútene synchronizujte údaje medzi aktívnou lokalitou a pohotovostnou lokalitou.
 - a. Prihláste sa do PowerEcho aktívnej lokality.
 - I. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.


NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero radiacích uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- II. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
 - b. Na PowerEcho vyberte z hlavnej ponuky **HA > Remote High Availability System > Manage DR System**.
 - c. V riadku, ktorý obsahuje systém DR s údajmi, ktoré sa majú synchronizovať, kliknite na . Vyberte smer synchronizácie údajov o produkte. Vykonajte operácie podľa pokynov.

NOTE

- Ak stavy primárnej lokality a sekundárnej lokality nepozostávajú z jedného aktívneho a jedného pohotovostného stavu, musíte zadať smer synchronizácie údajov o produkte a systém DR vykoná úplnú synchronizáciu na základe zadaného smeru. Napríklad, ak je určený smer z lokality A do lokality B, údaje lokality B sa prepíšu a údaje správy používateľov PowerEcho lokality B sa prepíšu údajmi lokality A o 00:00:00 hod. nasledujúci deň. Odporúčame vám špecifikovať produkt s najnovšími údajmi ako produkt aktívnej lokality, aby ste z neho synchronizovali údaje s produktom rovnocennej lokality.
- Ak je jedna z primárnej lokality a sekundárnej lokality aktívna a druhá je v pohotovostnom režime, nemusíte špecifikovať smer synchronizácie údajov o produkte. Systém automaticky synchronizuje údaje z aktívnej lokality do pohotovostnej lokality. Údaje o správe používateľov PowerEcho pohotovostnej lokality budú prepísané údajmi aktívnej lokality o 00:00:00 nasledujúceho dňa.

- d. Skontrolujte výsledok operácie. Ak výsledok operácie nie je taký, ako sa očakávalo, kontaktujte technickú podporu.
 - I. Na PowerEcho vyberte z hlavnej ponuky **HA > Remote High Availability System > Manage DR System**.
 - II. Skontrolujte, či je stav srdcového tepu medzi aktívnym miestom a miestom v pohotovostnom režime .
 - III. Skontrolujte, či je **Data Synchronization Status** všetkých produktov **Synchronized** alebo **Synchronizing**. Ak je **Data Synchronization Status Delayed**, medzi aktívnou lokalitou a pohotovostnou lokalitou sa synchronizuje veľké množstvo údajov. Po dokončení synchronizácie údajov skontrolujte stav.
 - IV. Overte si, že sa môžete prihlásiť do SmartPVMS aktívnej stránky.

3. Skontrolujte, či je alarm vymazaný.

- Ak áno, nie sú potrebné žiadne ďalšie kroky.
- Ak nie, zozbierajte informácie o manipulácii s alarmom a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-101201 Abnormálny srdcový tep

Popis alarmu

Tento alarm sa generuje, keď systém DR zistí (detekcia sa vykonáva každých 10 sekúnd), že buď aktívna lokalita, ani lokalita v pohotovostnom režime neprijíma správu srdcového tepu z lokality partnera v rámci prednastaveného trvania trikrát za sebou. Tento alarm sa automaticky vymaže, keď je srdcový tep medzi aktívnym miestom a miestom v pohotovostnom režime normálny.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101201	Kritické	Tlkot srdca

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Miesto 1	Názov lokality a adresa IP abnormálneho srdcového tepu na lokalite.
	Stránka 2	Názov lokality a adresa IP abnormálneho srdcového tepu na lokalite.

Vplyv na systém

Nie je možné vykonať prepnutie produktu, vynútenú synchronizáciu a vymazanie vzťahu replikácie údajov medzi aktívnou lokalitou a pohotovostnou lokalitou.

Možné príčiny

- Sieť srdcového tepu medzi aktívnym miestom a miestom v pohotovostnom režime je abnormálna.
- Služba DR aktívnej lokality a pohotovostnej lokality je abnormálna.
- Systémové certifikáty DR riadiacich uzlov na aktívnej lokalite a pohotovostnej lokalite sa nezhodujú alebo sú neplatné.

Postup

NOTE

Táto časť poskytuje iba základné metódy riešenia problémov. Ak chyba pretrváva aj po odstránení problémov pomocou tejto metódy, kontaktujte technickú podporu.

1. Skontrolujte, či je sieť srdcového tepu medzi aktívnym miestom a miestom v pohotovostnom režime normálna.
 - a. Použite PuTTY na prihlásenie do riadiaceho uzla na pohotovostnom mieste ako používateľ **sopuser** v režime SSH.
 - b. Spustíte nasledujúci príkaz na otestovanie pripojenia medzi riadiacimi uzlami na aktívnej lokalite a lokalite v pohotovostnom režime.
 - Pre adresu IPv4 spustíte nasledujúci príkaz:
> **ping** *heartbeat IP address of the management node at the active site*
 - Pre adresu IPv6 spustíte nasledujúci príkaz:
> **ping6** *heartbeat IP address of the management node at the active site*

NOTE

Ak je PowerEcho nasadené v režime klastra , odošlite príkaz ping Management0 a Management1 na partnerskej lokalite z Management0 a Management1. Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Dopyt na adresu IP správy uzla“ v *príručke správcu*.
Spustíte nasledujúce príkazy na Management0 v pohotovostnom režime:
> **ping** *heartbeat IP adresu Management0 na aktívnej stránke*
> **ping** *heartbeat IP adresu Management1 na aktívnej stránke*
Spustíte nasledujúce príkazy na Management1 v pohotovostnom režime:
> **ping** *heartbeat IP adresu Management0 na aktívnej stránke*
> **ping** *heartbeat IP adresu Management1 na aktívnej stránke*

Skontrolujte výstup príkazu.

- Ak sa zobrazia informácie podobné nasledujúcim, IP adresa môže byť testovaná a sieťové pripojenie je normálne:

```
64 bytes from heartbeat IP address of the management node at the active site: icmp_seq=1 ttl=251 time=42.1 ms
```

- Ak sa do 1 minúty nezobrazí žiadny príkaz, je sieťové pripojenie abnormálne. Spustíte nasledujúce príkazy na reštartovanie siete pohotovostnej lokality . Po reštartovaní siete znova skontrolujte konektivitu medzi riadiacimi uzlami na aktívnom mieste a pohotovostným miestom podľa 1.b. Ak je sieťové pripojenie stále abnormálne, kontaktujte správcu, aby skontroloval a obnovil sieť.

NOTE

Ak je PowerEcho nasadené v režime klastra , reštartujte sieť iba uzla, ktorý je v pohotovostnom režime a nedá sa testovať.

```
> su - root
```

```
Password: password for the root user
```

```
# systemctl restart network
```

```
# exit
```

- c. Stlačením **Ctrl+C** zastavíte príkaz **ping**.

2. Skontrolujte, či sú procesy DR riadiaceho uzla normálne na aktívnom mieste a na pohotovostnom mieste.

a. Prihláste sa do PowerEcho aktívnej lokality a pohotovostnej lokality .

I. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

II. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

b. Z hlavnej ponuky vyberte **Maintenance > Operation and Maintenance Management > Panoramic Monitoring**.

c. Na navigačnej table vyberte položku **Service Monitoring**.

d. V ľavom hornom rohu stránky **Service Monitoring** vyberte **CloudSOP-UniEP**.

e. Na karte **Processes** skontrolujte, či proces drmgrservice- x - x existuje a či je **Status** procesu **Running**.

NOTE

x označuje číslo inštancie. Vymeňte ho na základe požiadaviek lokality.

- Ak áno, procesy existujú a fungujú správne.
- Ak nie, kontaktujte technickú podporu.

f. V predchádzajúcich krokoch skontrolujte, či procesy DR existujú na pohotovostnom mieste. Ak je abnormálna, kontaktujte technickú podporu , aby obnovila procesy DR.

3. Skontrolujte, či nevypršala platnosť certifikátu systému DR riadiaceho uzla na aktívnej lokalite a lokalite v pohotovostnom režime.

Skontrolujte, či sa negeneruje alarm „ALM-51025 Certifikát systému DR vypršal“.

- Ak áno, aktualizujte systémový certifikát DR. Podrobnosti nájdete v časti „Odvzdávanie a aktualizácia certifikátov PowerEcho for Internal SmartPVMSCommunication“ v *príručke správcu*. Po úspešnom dokončení operácie prejdite na 5.
- Ak nie, táto chyba nie je spôsobená uplynutím platnosti certifikátu.

4. Skontrolujte, či je systémový certifikát DR riadiaceho uzla konzistentný medzi aktívnou lokalitou a pohotovostnou lokalitou.

- a. Porovnajete hodnotu SHA-256 certifikátu systému DR riadiaceho uzla medzi aktívnou lokalitou a pohotovostnou lokalitou.
- I. Použijete PuTTY na prihlásenie do riadiaceho uzla na aktívnom mieste ako používateľ **sopuser** v režime SSH.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 alebo Management1. Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Querying the Management IP Address of a Node“ v *Administrator Guide*.

- II. Ak chcete prepnúť na používateľa **ossadm**, spustíte nasledujúci príkaz:
> **su - ossadm**
- ```
Password: password for the ossadm user
```
- III. Ak chcete skontrolovať hodnotu SHA-256 certifikátu aktívnej lokality, spustíte nasledujúce príkazy:  
> **cd installation directory/manager/etc/ssl/dr**  
> **sha256sum server.cer trust.cer**  
Zobrazia sa informácie podobné týmto:
- ```
6bd440f7d4bfe363c99d729eb816b2d6a019d42cb3a659c6be514252b8904dee
server.cer
94be0a32258d4e14ee5c9fb9fb84ed354a00ce9c16fda11eb1d2948c705d6b77
trust.cer
```
- IV. Zopakujte kroky 4.a I. až 4.a. III. v riadiacom uzle na pohotovostnom mieste, aby ste skontrolovali hodnotu SHA-256 certifikátu pohotovostného miesta.
- Ak je hodnota medzi aktívnou lokalitou a pohotovostnou lokalitou konzistentná, systémové certifikáty DR aktívnej lokality a pohotovostnej lokality sa navzájom zhodujú a chyba nie je spôsobená nekonzistenciou certifikátov. V takom prípade kontaktujte technickú podporu.
 - Ak je hodnota nekonzistentná medzi aktívnou lokalitou a pohotovostnou lokalitou , systémový certifikát DR je nekonzistentný medzi aktívnou lokalitou a pohotovostnou lokalitou. Vykonajte 4.b až 4.g.

- b. Získajte súbory certifikátov z riadiaceho uzla na aktívnej lokalite.

- I. Spustíte nasledujúce príkazy na vytvorenie adresára **/tmp /cer1** a skopírujete súbory certifikátov do tohto adresára:
> **mkdir /tmp /cer 1**
> **cp installation directory/manager/etc/ssl/dr/* /tmp/cer1**
> **chgrp -R sopgroup /tmp /cer 1**
> **chmod 640 /tmp /cer1/***
- II. Pomocou FileZilla sa prihláste do riadiaceho uzla na aktívnej lokalite ako používateľ **sopuser** a stiahnite si súbory certifikátov v adresári **/tmp /cer 1** do svojho počítača.

Súbory certifikátov:

- manifest.json
- server.cer
- server.jks
- server_key.pem
- dôverovať.cer

- c. Použite PuTTY na prihlásenie do riadiaceho uzla na pohotovostnom mieste ako používateľ **sopuser** v režime SSH.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 a potom na Management1 . Podrobnosti o tom, ako získať adresu IP uzla, nájdete v časti „Querying the Management IP Address of a Node „ v *Administrator Guide*.

- d. Nahrajte získané súbory certifikátov do *inštalačného adresára* **/manager/etc/ssl/dr** v uzle správy na pohotovostnom mieste.
- Spustite nasledujúci príkaz na vytvorenie dočasného adresára **/tmp/cer 2** na ukladanie súborov certifikátov:
> mkdir /tmp/cer 2
 - Pomocou FileZilla sa prihláste do riadiaceho uzla na pohotovostnom mieste ako používateľ **sopuser** a nahrajte súbory certifikátov získané v 4.b.ii do adresára **/tmp/cer 2**.
 - Ak chcete prepnúť na používateľa **ossadm** , spustite nasledujúci príkaz:
> su - ossadm

```
Password: password for the ossadm user
```
 - Spustite nasledujúci príkaz na skopírovanie súborov certifikátov z adresára **/tmp/cer 2** do *inštalačného adresára* **/manager/etc/ssl/dr**: **> cp /tmp/cer2/* installation directory/manager/etc/ssl/dr**
- e. Spustite nasledujúci príkaz na nastavenie povolenia pre súbory certifikátov:
> find installation directory/manager/etc/ssl/dr -type f | xargs chmod 600
- f. Spustite nasledujúce príkazy na reštartovanie DRMgrService:
> source installation directory/manager/bin/engr_profile.sh
> ipmc_adm -cmd restartapp -tenant manager -app DRMgrService
Ak sa zobrazia nasledujúce informácie, spustí sa služba DRMgrService. V opačnom prípade kontaktujte technickú podporu.

```
Stopping process drmgrservice-0-0 ... success  
Starting process drmgrservice-0-0 ... success
```
- g. Odstráňte dočasný súbor.
- Spustite nasledujúce príkazy na odstránenie dočasných súborov v uzle správy na aktívnom mieste a prepnutie na používateľa **sopuser**:
> cd /tmp

```
> rm -rf cer 1
```

```
> výstup
```

II. Spustíte nasledujúce príkazy, aby ste odstránili dočasné súbory v riadiacom uzle na pohotovostnom mieste a prepli na používateľa **sopuser**:

```
> exit
```

```
> cd /tmp
```

```
> rm -rf cer 2
```

5. Skontrolujte, či je alarm vymazaný.

- Ak áno, nie sú potrebné žiadne ďalšie kroky.
- Ak nie, zozbierajte informácie o manipulácii s alarmom a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-101205 Zlyhanie plánovaného zálohovania údajov o produkte

Popis alarmu

Ak je naplánovaná úloha na zálohovanie údajov o produkte čiastočne úspešná alebo zlyhá, PowerEcho ohlásí alarm „Product Data Scheduled Backup Failure“. Tento alarm sa automaticky vymaže, keď sa úloha zálohovania úspešne vykoná.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101205	Kritické	Stav zálohy

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Alias produktu	Alias produktu.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.

Vplyv na systém

Naplánovaná úloha na zálohovanie údajov produktu sa nepodarí vykonať a bude ovplyvnená obnova údajov.

Možné príčiny

- Parametre zálohovania nie sú nakonfigurované.
- Záložné údaje sa nepodarilo uložiť na záložný server.
- Zálohovanie údajov produktu zlyhalo alebo čiastočne zlyhalo.

Postup

Vyberte zodpovedajúci postup odstraňovania problémov v tabuľke 1 na základe príčiny zlyhania zálohovania.


Tabuľka 1 Postup pri odstraňovaní zlyhaní zálohovania

Príčina	Postup
Parametre zálohovania nie sú nakonfigurované.	Podrobnosti nájdete v „Nastavenie parametrov zálohovania“.
Záložné údaje sa nepodarilo uložiť na záložný server.	Podrobnosti nájdete v „Kontrola konektivity a úložného priestoru záložného servera“.
Zálohovanie údajov produktu zlyhalo alebo čiastočne zlyhalo.	Podrobnosti nájdete v časti „Zobrazenie podrobností o úlohe“.

- Nastavenie parametrov zálohovania

1. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**.
 3. Na stránke **Configure Backup Parameters** vykonajte operácie podľa výzvy.
 4. Vytvorte úlohu na zálohovanie príslušných údajov o produkte na základe podrobností o alarme.
 - a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Product Data**.
 - b. Na stránke **Back Up Product Data** vykonajte operácie podľa výzvy.
 - c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
 - Ak je úloha zálohovania úspešná, prejdite na 5.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.
 5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

- Kontrola konektivity a úložného priestoru záložného servera

1. Použijete PuTTY na prihlásenie do ľubovoľného databázového uzla PowerEcho ako používateľ **sopuser**.

2. Ak chcete prepnúť na používateľa **ossadm**, spustíte nasledujúci príkaz:
> **su - ossadm**

```
Password: password for the ossadm user
```


3. Spustíte nasledujúci príkaz na kontrolu konektivity medzi databázovým uzlom a záložným serverom:

```
> sftp backup server username@[IP address of the backup server]
```

```
Backup server username@IP address of the backup server's password:
```

- Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Prejdite na 4.

```
Connected to IP address of the backup server
sftp>
```

- Ak sa zobrazia informácie podobné nasledujúcim, autentifikácia odtlačkom prsta medzi uzlom databázy a záložným serverom sa stratí alebo nebola nakonfigurovaná. Na PowerEcho vyberte z hlavnej ponuky **Zálohovanie a obnovenie > Konfigurácia > Konfigurovať parametre zálohovania**. V oblasti **Záložný server** kliknutím  prekonfigurujte odtlačok SFTP. Po úspešnej operácii prejdite na 4. Ak operácia zlyhá, kontaktujte technickú podporu.

```
The authenticity of host '10.10.10.28 (10.10.10.28)' can't be
established.
```

```
...
```

```
No matching host key fingerprint found in DNS.
```

- Keď sa zobrazia nasledujúce informácie, stlačením klávesov **Ctrl + C** ukončíte zobrazovanie informácií o autentifikácii odtlačkom prsta SFTP. Ak sa vráti chyba časového limitu požiadavky, sieťové pripojenie je abnormálne. Skontrolujte a obnovte sieťové pripojenie. Po úspešnej operácii prejdite na 4. V opačnom prípade kontaktujte technickú podporu.

```
Are you sure you want to continue connecting (yes/no)?
```

4. Použijete PuTTY na prihlásenie na záložný server ako používateľ záložného servera v režime SSH.

NOTE

- Používateľ na prihlásenie na záložný server musí mať povolenie SSH. V opačnom prípade kontaktujte správcu servera, aby používateľovi pridelil povolenie.
- Ak sa riadiaci uzol používa ako záložný server, prihláste sa na záložný server ako používateľ **sopuser** v režime SFTP a potom prepnite na používateľa záložného servera.

- Ak je prihlásenie úspešné, heslo sa nezmení a záložný server funguje správne. Prejdite na 5.
- Ak prihlásenie zlyhalo, možnou príčinou je zmena hesla, vypršala platnosť hesla alebo je chybný záložný server. Kontaktujte personál O&M.

5. Skontrolujte miesto na záložnom serveri.

- a. Spustíte nasledujúci príkaz, aby ste skontrolovali dostupné miesto na záložnom serveri:

```
> df -Ph
```


- b. Zobrazia sa informácie podobné nasledujúcim. Skontrolujte hodnotu **Avail** v stĺpci **Mounted on** riadku, ktorý obsahuje oddiel zdieľaného adresára SFTP na záložnom serveri.

```
Filesystem          Size  Used Avail Use% Mounted on
/dev/xxx/oss_vg-opt_vol 53G  27G  24G  54% /xxx
...
```

- c. Skontrolujte, či veľkosť zostávajúceho priestoru zálohy spĺňa požiadavky na súbor zálohy. V nasledujúcom texte sa predpokladá, že veľkosť záložného súboru je 5 GB.
- Ak je zostávajúci priestor zálohy väčší ako 5 GB, prejdite na 6.
 - Ak je zostávajúci priestor zálohy menší alebo rovný 5 GB, kontaktujte správcu, aby ukladací priestor rozšíril.

6. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

7. Vytvorte úlohu na zálohovanie príslušných údajov o produkte na základe podrobností o alarme.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Product Data**.
- b. Na stránke **Back Up Product Data** vykonajte operácie podľa výzvy.
- c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
- Ak je úloha zálohovania úspešná, prejdite na 8.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

8. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, kontaktujte technickú podporu.

- Zobrazenie podrobností o úlohe

1. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

2. Na PowerEcho vyberte **System > Task List** z hlavnej ponuky.

3. Kliknutím > získate **Location Info** o zlyhanej naplánovanej úlohe na zálohovanie údajov o produkte a opravte poruchu na základe **Location Info**. Ak je porucha odstránená, prejdite na 4 . V opačnom prípade kontaktujte technickú podporu .

4. Vytvorte úlohu na zálohovanie príslušných údajov o produkte na základe podrobností o alarme.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Product Data**.

- b. Na stránke **Back Up Product Data** vykonajte operácie podľa výzvy.

- c. Z hlavnej ponuky vyberte **System > Task List** . Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.

- Ak je úloha zálohovania úspešná, prejdite na 5.
- Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-101206 Kanál správy SSH je chybný

Popis alarmu

Tento alarm sa generuje, keď PowerEcho zistí (detekcia sa vykonáva každých 180 sekúnd), že spojenie SSH medzi riadiacim uzlom a produktovým uzlom je tri po sebe idúce časy abnormálne. Tento alarm sa automaticky vymaže, keď sa obnoví spojenie SSH medzi riadiacim uzlom a produktovým uzlom.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101206	Kritické	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

PowerEcho nemôže spravovať zodpovedajúce uzly, čo ovplyvňuje panoramatické monitorovanie a funkcie zálohovania a obnovy zodpovedajúcich uzlov.

Možné príčiny

- Stav uzla produktu je abnormálny.
- Sieťové pripojenie medzi riadiacim uzlom a produktovým uzlom je abnormálne.
- Platnosť hesla pre používateľa **ossadm** uzla produktu vypršala.
- Vzťah dôvery SSH medzi riadiacim uzlom a produktovým uzlom je poškodený.

Postup

1. Skontrolujte, či stav uzla ALM-101208 je Abnormálny alarm existuje a či sú hodnoty **Host** ALM-101206 a ALM-101208 rovnaké.
 - Ak áno, riešte chybu *ALM-101208 Node status is Abnormal*.
 - Ak nie, prejdite na 2.

2. Použijte PuTTY na prihlásenie do riadiaceho uzla ako používateľ **sopuser** v režime SSH.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 a potom na Management1.

3. Ak chcete prepnúť na používateľa **ossadm**, spustite nasledujúci príkaz:

su - ossadm

```
Password: password for the ossadm user
```

4. Spustite nasledujúci príkaz a otestujte konektivitu **SSH** medzi riadiacim uzlom a produktovým uzlom.

ssh node IP address in the alarm parameters

NOTE

Ak je uzol určený parametrom **Host** v parametroch alarmu riadiacim uzlom, môžete sa prihlásiť do riadiaceho uzla a otestovať pripojenie SSH k akémukoľvek uzlu produktu.

- Ak sa môžete prihlásiť do ľubovoľného produktového uzla bez zadania hesla, vzťah dôvery SSH medzi riadiacim uzlom a produktovým uzlom je normálny. Prejdite na 5.
- Ak sa zobrazia nasledujúce informácie, heslo používateľa **ossadm** uzla je neplatné. Aktualizujte heslo podľa časti „Zmena hesiel pre používateľov OS“ v príručke správcu a potom znova otestujte pripojenie SSH medzi uzlom správy a uzlom produktu.

```
WARNING: Your password has expired.
```

NOTE

Heslo používateľa **ossadm** v uzle produktu musí byť rovnaké ako heslo používateľa **ossadm** v uzle správy.

- Ak sa vyžaduje heslo pre užívateľa **ossadm**, vzťah dôvery SSH medzi riadiacim uzlom a uzlom produktu je abnormálny. Na obnovenie vzťahu dôveryhodnosti SSH vykonajte nasledujúce operácie:
 - a. Ak chcete ukončiť aktuálnu operáciu, stlačte **Ctrl + C**.
 - b. Ak chcete prepnúť na používateľa **root**, spustite nasledujúci príkaz:

su - root

```
Password: password for the root user
```
 - c. Skontrolujte konfiguráciu brány firewall.
 - Pre adresu IPv4 spustite nasledujúci príkaz:

iptables -L
 - Ak je adresa IP adresou IPv6, spustite nasledujúci príkaz:

ip6tables -L

Skontrolujte, či hodnota **source Chain INPUT (policy ACCEPT)** vo výstupe príkazu obsahuje IP adresu uzla v parametroch alarmu.

```
...
Chain INPUT (policy ACCEPT)
target     prot opt source                               destination
...
```

- Ak áno, prejdite na 4.d.
 - Ak nie, prejdite na 4.f.
- d. Odstráňte pravidlá konfigurácie brány firewall.
- Pre adresu IPv4 spustite nasledujúci príkaz:
iptables -D INPUT -s *node IP address in the alarm parameters* -j DROP
 - Ak je adresa IP adresou IPv6, spustite nasledujúci príkaz:
ip6tables -D INPUT -s *node IP address in the alarm parameters* -j DROP
- e. Spustením nasledujúcich príkazov prepnete späť na používateľa **ossadm** a znova otestujte pripojenie SSH medzi riadiacim uzlom a produktovým uzlom:
- exit**
ssh *node IP address in the alarm parameters*
- Ak sa môžete prihlásiť do ľubovoľného produktového uzla bez zadania hesla, vzťah dôvery SSH medzi riadiacim uzlom a produktovým uzlom je normálny. Prejdite na 5. V opačnom prípade kontaktujte technickú podporu.

NOTE

Ak je uzol určený parametrom **Host** v parametroch alarmu riadiacim uzlom, môžete sa prihlásiť do riadiaceho uzla a otestovať pripojenie SSH k akémukoľvek uzlu produktu.

- f. Spustíte nasledujúci príkaz na otvorenie súboru **id_rsa.pub** riadiaceho uzla:
cat *home directory of the ossadm user*/.ssh/id_rsa.pub
- g. Skopírujte obsah súboru **id_rsa.pub** do lokálneho počítača pre ďalšie operácie.
- h. Použite PuTTY na prihlásenie do uzla s dôveryhodným vzťahom SSH, ktorý sa má obnoviť, ako používateľ **sopuser** v režime SSH.

NOTE

- Ak je uzol určený parametrom **Host** v parametroch alarmu riadiaci uzol a PowerEcho je nasadené v režime klastra, musíte sa prihlásiť do riadiacich uzlov okrem tých v 2.
 - Ak je uzol určený parametrom **Host** v parametroch alarmu uzlom produktu, musíte sa prihlásiť do uzla produktu.
- i. Ak chcete prepnúť na používateľa **ossadm**, spustite nasledujúci príkaz:
su - ossadm

```
Password: password for the ossadm user
```

- j. Spustíte nasledujúci príkaz na pridanie obsahu získaného v 4.g na koniec súboru **authorized_keys**:
echo "content copied from the id_rsa.pub file" >> /home directory of the ossadm user/.ssh/authorized_keys

Znova otestujte pripojenie SSH medzi riadiacim uzlom a produktovým uzlom.

5. Počkajte 3 minúty (doba detekcie je 180 sekúnd) a skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Alarm nie je možné automaticky vymazať v nasledujúcich prípadoch. Musíte manuálne vymazať alarm na oboch SmartPVMS a PowerEcho. Ak chcete vymazať alarm na PowerEcho, vyberte **Maintenance > Operation and Maintenance Management > Exceptions and Events** a kliknite na **Clear** v stĺpci **Operation** pri alarme nakarte **Exceptions**.

- Názov uzla, pre ktorý sa generuje tento alarm, sa zmenil.
- Server, pre ktorý sa generuje tento alarm, už nie je monitorovaný.

ALM-101207 Zlyhanie príjmu alarmov v dôsledku odpojenia zariadenia

Popis alarmu

Tento alarm sa generuje, keď PowerEcho zistí (každá perióda detekcie trvá 5 minút a detekcia sa vykoná trikrát v intervale 5 sekúnd počas každej periódy), že spojenie medzi riadiacim uzlom a zariadením (napríklad serverom alebo diskové pole) sa preruší trikrát za sebou. Tento alarm sa automaticky vymaže, keď PowerEcho zistí, že spojenie medzi riadiacim uzlom a zariadením je obnovené.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101207	Kritické	Komunikačný alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	IP adresa	IP adresa zariadenia.
	Typ zariadenia	Typ zariadenia.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.

Vplyv na systém

Pri prijímaní poplachu príslušného zariadenia cez PowerEcho a pri nahlasovaní poplachu do SmartPVMS dochádza k zlyhaniu. Výsledkom je, že zdravotný stav servera, diskového poľa alebo prepínača nie je možné získať včas.

Možné príčiny

- Sieťové pripojenie medzi riadiacim uzlom a zariadením je abnormálne.
- Overovacie heslo alebo šifrovacie heslo pre používateľa SNMP zariadenia je nesprávne.

Postup

1. Použite PuTTY na prihlásenie do riadiaceho uzla ako používateľ **sopuser** v režime SSH.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

2. Ak chcete prepnúť na používateľa **ossadm** , spustíte nasledujúci príkaz:

> **su - ossadm**

```
Password: password for the ossadm user
```

3. Otestujte sieťové pripojenie medzi riadiacim uzlom a zariadením.

a. Spustíte nasledujúci príkaz, aby ste získali IP adresu portu načúvajúceho alarmovej služby a poznačte si IP adresu:

> **netstat -anp |grep 30085**

Zobrazia sa informácie podobné nasledujúcim. **10.10.10.10** je IP adresa načúvacieho portu alarmovej služby.

```
udp        0          0 10.10.10.10:30085  0.0.0.0:*          146108/java
```

b. Skontrolujte sieťové pripojenie:

- Ak je adresa IP adresou IPv4, spustíte nasledujúci príkaz:
> **ping -I IP address of the alarm service listening port IP address of the device**
- Ak je adresa IP adresou IPv6, spustíte nasledujúci príkaz:
> **ping6 -I IP address of the alarm service listening port IP address of the device**

Vykonajte operácie na základe výstupu príkazu.

- Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Stlačením **Ctrl + C** zastavte príkaz a prejdite na 4.

```
64 bytes from IP address of the device: icmp_seq=1 ttl=61 time=3.06 ms
```

- V iných prípadoch je sieťové pripojenie abnormálne. Stlačte **Ctrl + C** na zastavenie príkazu. Skontrolujte a obnovte sieťové pripojenie.

Počkajte 5 minút a skontrolujte, či je alarm vymazaný. Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky. Ak alarm pretrváva, prejdite na 4.

4. Prekonfigurujte overovacie heslo alebo šifrovacie heslo pre používateľa SNMP.

a. Prihláste sa do PowerEcho.


- I. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- II. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

b. Na PowerEcho vyberte z hlavnej ponuky **Infrastructure > Hardware Management > Configure Server Alarm Receiving Parameters or Infrastructure > Hardware Management > Configure Disk Array Alarm Receiving Parameters** z hlavného menu podľa typu zariadenia.

- c. Kliknite  na stĺpec **Operation** v riadku, ktorý obsahuje IP adresu príslušného zariadenia, a zadajte získané overovacie heslo alebo šifrovacie heslo pre používateľa SNMP.
- d. Kliknite na tlačidlo **Apply**.

Vymazanie alarmu

ADAC : PowerEcho kontroluje stav pripojenia medzi riadiacim uzlom a zariadením každých 5 minút. Tento alarm sa automaticky vymaže, keď je pripojenie normálne.

ALM-101208 Stav uzla je Abnormálny

Popis alarmu

Tento alarm sa generuje, keď PowerEcho zistí (detekcia sa vykonáva každých 60 sekúnd), že uzol je nedostupný 8 krát po sebe idúcich opakovaníach. Tento alarm sa automaticky vymaže, keď sa uzol obnoví.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101208	Major	Komunikačný alarm

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

Nemôžete sa prihlásiť do uzla alebo sa pri vykonávaní operácií na uzle môže vyskytnúť chyba.

Možné príčiny

- OS uzla sa nedá prihlásiť alebo sa nevráti žiadna odpoveď.
- Uzol je vypnutý alebo je sieťové pripojenie uzla abnormálne.
- Proces DeployAgent v uzle je abnormálny.
- Platnosť IR certifikátu uzla vyprší a interná komunikácia je abnormálna.
- Ak v uzle existuje databáza, stav replikácie inštancií databázy môže byť abnormálny. V dôsledku toho je uzol abnormálny.

Postup

1. Vykonajte položky kontroly a metódy kontroly uvedené v tabuľke 1 a opravte poruchy podľa zodpovedajúcich metód odstraňovania problémov.

NOTE

Zlyhanie uzla je spôsobené komplikovanými príčinami. Táto časť obsahuje základné metódy riešenia problémov na odstránenie poruchy. Ak porucha pretrváva aj po vykonaní nasledujúcich operácií, zozbierajte informácie o poruche a kontaktujte technickú podporu.

Tabuľka 1 Riešenie problémov s chybami uzla produktu

Č.	Skontrolujte položku	Metóda kontroly	Metóda pre odstránenie
1	Sieťové pripojenie	Obráťte sa na správcu, aby skontroloval, či je sieťové pripojenie normálne.	Ak chcete obnoviť sieťové pripojenie, kontaktujte správcu.
2	Stav prevádzky virtuálnych počítačov alebo fyzických počítačov	Kontaktujte správcu, aby skontroloval, či sú virtuálne počítače alebo fyzické počítače abnormálne, napríklad či sú virtuálne počítače alebo fyzické počítače vypnuté alebo odstránené.	Ak chcete reštartovať a obnoviť virtuálne počítače alebo fyzické počítače, kontaktujte správcu.
3	Stav spustenia OS	<ol style="list-style-type: none"> Reštartujte OS. Použite PuTTY na prihlásenie sa do chybného uzla ako používateľ sopuser v režime SSH. 	Ak prihlásenie zlyhá alebo sa nevráti žiadna odpoveď, operačný systém chybného uzla je abnormálny. Obnovte operačný systém chybného uzla. Podrobnosti nájdete v časti „Obnovenie operačného systému produktového uzla“ v príručke správcu.
4	Spustený stav procesu ServiceAwareWatchAgent process	<ol style="list-style-type: none"> Použite PuTTY na prihlásenie sa do chybného uzla ako používateľ sopuser v režime SSH. Ak chcete prepnúť na používateľa ossadm, spustíte nasledujúci príkaz: sú - ossadm <pre> Password: password for the ossadm user </pre> <p>Spustíte nasledujúce príkazy, aby ste skontrolovali, či proces DeployAgent beží správne:</p> <pre> source installation directory /manager/bin/engr_profile.sh ipmc_admin -cmd statusapp -app ServiceAwareWatchAgent </pre> <pre> ossadm 321431 1 5 11:45 ? 00:27:26 installation </pre>	<p>Ak proces Service Aware Watch Agent nie je spustený, spustíte ho spustením nasledujúcich príkazov:</p> <p>Zdrojový inštalčný adresár /manager/bin/engr_profile.sh</p> <p>ipmc_admin -cmd startapp -app ServiceAwareWatchAgent - správca nájomníkov</p> <p>Ak sa zobrazia nasledujúce informácie, proces Service Aware Watch Agent sa úspešne spustí. V opačnom prípade kontaktujte technickú podporu.</p>

Tabuľka 1 Riešenie problémov s chybami uzla produktu

Č.	Skontrolujte položku	Metóda kontroly	Metóda pre odstránenie
		<pre>directory/manager/agent/DeployAgent /rtsp/python/bin/python installation directory/manager/apps/DeployAgent- 21.20.8/tools/pyscript/deployagent/ DeployAgent.pyc -DNFW=deployagent ...</pre> <p>2. Ak je na výstupe príkazu Status RUNNING, proces sa spustí.</p> <p>3. Ak je na výstupe príkazu Status STOPPED, proces sa zastaví.</p>	<pre>Starting process serviceawarewatchagent-0-0 ... success</pre>
5	IR certifikát	<p>1. Použite PuTTY na prihlásenie sa do chybného uzla ako používateľ sopuser v režime SSH.</p> <p>2. Ak chcete prepnúť na používateľa ossadm, spustíte nasledujúci príkaz: > su - ossadm</p> <pre>Password: password for the ossadm user</pre> <p>3. Spustíte nasledujúce príkazy na kontrolu platnosti IR certifikátu: inštalačný adresár cd /manager /etc/ssl/internal openssl x509 -in server.cer -noout -dates</p> <p>Ak sa zobrazia informácie podobné nasledujúcim, čas zobrazený napravo od notAfter je čas vypršania platnosti IR certifikátu:</p> <pre>notBefore=18. októbra 00:00:00 2018 GMT notAfter=13. októbra 00:00:00 2038 GMT</pre> <ul style="list-style-type: none"> • Ak platnosť IR certifikátu vypršala, aktualizujte certifikát CA. • Ak je IR certifikát platný, chyba nie je spôsobená expiráciou certifikátu. 	Aktualizujte certifikát CA. Podrobnosti nájdete v časti „Správa certifikátov CA“ v príručke správcu.
6	Stav replikácie databázy	Podrobnosti nájdete v ALM-101210 Stav lokálnej kópie databázy je abnormálny.	Podrobnosti nájdete v ALM-101210 Stav lokálnej kópie databázy je abnormálny.

2. Prihláste sa do PowerEcho.

a. Prístup k PowerEcho získate na [https://klientskej IP adrese PowerEcho : 31945](https://klientskejIPadresePowerEcho:31945).

NOTE

Ak je PowerEcho nasadené v režime klastra, prihláste sa do riadiaceho uzla pomocou jeho pohyblivej adresy IP.

b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

3. Na PowerEcho vyberte z hlavnej ponuky **Maintenance > Operation and Maintenance Management > Panoramic Monitoring**.

4. Na navigačnej table vyberte položku **Node Monitoring**.

5. V ľavom hornom rohu stránky **Node Monitoring** vyberte produkt zodpovedajúci hodnote parametra alarmu **Product alias**.

6. V oblasti **Node List** skontrolujte stav uzla na základe adresy IP uvedenej v časti **Other Information**.

- Ak je stav obnoveného uzla normálny, porucha sa odstráni.
- Ak je stav obnoveného uzla stále abnormálny, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Tento alarm nie je možné vymazať automaticky a je potrebné ho vymazať manuálne v nasledujúcich situáciách:

- Zmení sa názov uzla, pre ktorý sa tento alarm generuje.
- Server, pre ktorý sa generuje tento alarm, nie je monitorovaný.

ALM-101210 Stav lokálnej kópie databázy je abnormálny

Popis alarmu

Tento alarm sa generuje, keď PowerEcho zistí (každá detekčná perióda trvá 100 sekúnd), že replikácia medzi inštanciami hlavnej a podriadenej databázy je abnormálna sedemkrát za sebou. Tento alarm sa automaticky vymaže, keď je stav replikácie databázy normálny.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101210	Major	Alarm chyby spracovania

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Hostiteľ	Názov chybného uzla.
	Operačný systém	Operačný systém servera.
	Databázová služba	Názov inštancie databázy, pre ktorú sa generuje alarm.
	Typ databázy	Typ databázy, pre ktorú sa generuje alarm.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	IP adresa	IP adresa chybného uzla.
	Alias produktu	Alias produktu, pre ktorý sa generuje alarm.

Vplyv na systém

Abnormálny stav lokálnej replikácie medzi master a slave databázami spôsobuje nekonzistenciu údajov medzi databázami. Ak abnormálny stav pretrváva dlhší čas, sú ovplyvnené služby.

Možné príčiny

- Komunikácia medzi uzlami, kde sa nachádzajú inštancie hlavnej a podriadenej databázy, je abnormálna.
- Replikačný vzťah je nesprávny.
- Miesto na disku je plné.

Postup

1. Použite PuTTY na prihlásenie do riadiaceho uzla ako používateľ **sopuser** v režime SSH.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, vykonajte operácie na Management0 alebo Management1.

2. Ak chcete prepnúť na používateľa **ossadm** , spustite nasledujúci príkaz:

su - ossadm

```
Password: password for the ossadm user
```

3. Ak chcete zistiť stav replikácie inštancie databázy, spustite nasledujúce príkazy.

```
cd inštalačný adresár /manager/apps/DBAgent/bin/  
bash dbsvc_adm -cmd query-db-instance
```

Zobrazia sa informácie podobné týmto:

```
DBInstanceId ... Port IP ... Rola Stav Rpl ...  
apmdbContext-10_90_73_163-3@10_90_73_164-3 ... 10.90.73.164 32082 ... Slave  
Normal ...  
apmdbContext-10_90_73_178-21@10_90_73_179-21 ... 10.90.73.179 32080 ... Slave  
Abnormal (101) ...  
apmdbContext-10_90_73_178-21@10_90_73_179-21 ... 10.90.73.179 32080 ... Slave  
Abnormal (103) ...  
...
```

- Ak je hodnota **Rpl Status --** , inštancia databázy je jedna inštancia. Prejdite na 8.
 - Ak je hodnota **Rpl Status Normal**, stav replikácie inštancie databázy je normálny. Prejdite na 8.
 - Ak je hodnota **Rpl Status Building**, inštancia podriadenej databázy sa prestavuje a všetky údaje inštancie hlavnej databázy sa násilne synchronizujú s inštanciou podriadenej databázy. Počkejte, kým hodnota **Rpl Status** nebude **Normal**, a prejdite na 8.
 - Ak je hodnota **Rpl Status Delay**, podriadená databáza synchronizuje údaje z inštancie hlavnej databázy. Počkejte, kým hodnota **Rpl Status** nebude **Normal**, a prejdite na 8.
 - Ak je hodnota **Rpl Status Abnormal**, stav replikácie databázy je abnormálny. Zaznamenajte kód chyby do zátvoriek napravo od položky **Abnormal**. Prejdite na 4.
4. Ak chcete skontrolovať miesto na disku databázy, spustite nasledujúci príkaz:

df -h

Ako je znázornené v nasledujúcom výstupe príkazu, priestor oddielu **/opt** , kde sa nachádza adresár databázy **/opt/redis** alebo **/opt/zenith** , je 0. Včas vyčistite priestor.

```
Filesystem                Size  Used Avail Use% Mounted on  
... ..  
/dev/mapper/vg_root-lv_opt 498G 498G  0   100% /opt  
tmpfs                     5.9G   0   5.9G   0% /run/user/3001  
tmpfs                     5.9G   0   5.9G   0% /run/user/0
```

Skontrolujte, či je miesto na disku databázy vyčerpané.

- Ak áno, prejdite na 5.
- Ak nie, kontaktujte technickú podporu.

5. Ak chcete prepnúť na používateľa **root**, spustíte nasledujúci príkaz:

su - root

```
Password: password for the ossadm user
```

6. Ak chcete odstrániť historické súbory, spustíte nasledujúci príkaz:

NOTE

Vyčistenie miesta na disku je riskantná operácia. Pred odstránením historických súborov si najprv zálohujte súbory alebo priečinky, ktoré chcete odstrániť. Pri vykonávaní tejto operácie buďte opatrní.

```
rm -r historické súbory
```

7. Spustíte nasledujúci príkaz na ukončenie od používateľa **root**:

exit

8. Počkajte 2 minúty a potom skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, získajte informácie o spracovaní alarmu a kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

Tento alarm nie je možné vymazať automaticky a je potrebné ho vymazať manuálne v nasledujúcich situáciách:

- Zmení sa názov uzla, pre ktorý sa tento alarm generuje.
- Server, pre ktorý sa generuje alarm, nie je monitorovaný.

ALM-101216 Plánované zlyhanie zálohovania

Popis alarmu

Ak naplánovaná úloha na zálohovanie PowerEcho zlyhá, PowerEcho ohlásí alarm „Scheduled Backup Failure“. Tento alarm sa automaticky vymaže, keď sa úloha zálohovania úspešne vykoná.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101216	Kritické	Stav zálohy

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Alias produktu	Alias produktu.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.
Ďalšie informácie	Záložný objekt	PowerEcho

Vplyv na systém

Naplánovaná úloha na zálohovanie PowerEcho sa nepodarí vykonať a bude to mať vplyv na obnovenie údajov.

Možné príčiny

- Parametre zálohovania nie sú nakonfigurované.
- Záložné údaje sa nepodarilo uložiť na záložný server.
- PowerEcho sa nepodarilo zálohovať.

Postup

Vyberte zodpovedajúci postup odstraňovania problémov v tabuľke 1 na základe príčiny zlyhania zálohovania.

Tabuľka 1 Postup pri odstraňovaní zlyhaní zálohovania

Príčina	Postup
Parametre zálohovania nie sú nakonfigurované.	Podrobnosti nájdete v časti „Nastavenie parametrov zálohovania“


Tabuľka 1 Postup pri odstraňovaní zlyhaní zálohovania

Príčina	Postup
Záložné údaje sa nepodarilo uložiť na záložný server.	Podrobnosti nájdete v časti „Kontrola konektivity a úložného priestoru záložného servera“.
PowerEcho sa nepodarilo zálohovať.	Podrobnosti nájdete v časti „Zobrazenie podrobností o úlohe“

- Nastavenie parametrov zálohovania

1. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**.
 3. Na stránke **Configure Backup Parameters** vykonajte operácie podľa výzvy.
 4. Vytvorte úlohu na zálohovanie PowerEcho.
 - a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up the Management Plane**.
 - b. Na zobrazenej stránke vykonajte operácie podľa výzvy.
 - c. Z hlavnej ponuky vyberte **System > Task List** . Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
 - Ak je úloha zálohovania úspešná, prejdite na 5.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.
 5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

- Kontrola konektivity a úložného priestoru záložného servera

1. Použijete PuTTY na prihlásenie do ľubovoľného databázového uzla PowerEcho ako používateľ **sopuser** v režime SSH.

2. Ak chcete prepnúť na používateľa **ossadm**, spustíte nasledujúci príkaz:
> **su - ossadm**

```
Password: password for the ossadm user
```


3. Spustíte nasledujúci príkaz na kontrolu konektivity medzi databázovým uzlom a záložným serverom:

sftp *používateľské meno záložného servera@[IP adresa hesla záložného servera]*

```
Backup server username@IP address of the backup server's password:
```

- Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Prejdite na 4.

```
Connected to IP address of the backup server  
sftp>
```

- Ak sa zobrazia informácie podobné nasledujúcim, autentifikácia odtlačkom prsta medzi uzlom databázy a záložným serverom sa stratí alebo nebola nakonfigurovaná. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**. V oblasti **Backup server** kliknutím  prekonfigurujte odtlačok SFTP. Po úspešnej operácii prejdite na 4. Ak operácia zlyhá, kontaktujte technickú podporu.

```
The authenticity of host '10.10.10.28 (10.10.10.28)' can't be  
established.  
...  
No matching host key fingerprint found in DNS.
```

- Keď sa zobrazia nasledujúce informácie, stlačením klávesov **Ctrl + C** ukončíte zobrazovanie informácií o autentifikácii odtlačkom prsta SFTP. Ak sa vráti chyba časového limitu požiadavky, sieťové pripojenie je abnormálne. Skontrolujte a obnovte sieťové pripojenie. Po úspešnej operácii prejdite na 4. V opačnom prípade kontaktujte technickú podporu.

```
Are you sure you want to continue connecting (yes/no)?
```

4. Použijete PuTTY na prihlásenie na záložný server ako používateľ záložného servera v režime SSH.

NOTE

- Používateľ na prihlásenie na záložný server musí mať povolenie SSH. V opačnom prípade kontaktujte správcu servera, aby používateľovi pridelil povolenie.
- Ak sa riadiaci uzol používa ako záložný server, prihláste sa na záložný server ako používateľ **sopuser** v režime SFTP a potom prepnite na používateľa záložného servera.

- Ak je prihlásenie úspešné, heslo sa nezmení a záložný server funguje správne. Prejdite na 5.

- Ak prihlásenie zlyhalo, možnou príčinou je zmena hesla, vypršala platnosť hesla alebo je chybný záložný server. Kontaktujte personál O&M.

5. Skontrolujte miesto na záložnom serveri.

- a. Spustíte nasledujúci príkaz, aby ste skontrolovali dostupné miesto na záložnom serveri:

> **df -Ph**


- b. Zobrazia sa informácie podobné nasledujúcim. Skontrolujte hodnotu **Avail** v stĺpci **Mounted on** riadku, ktorý obsahuje oddiel zdieľaného adresára SFTP na záložnom serveri.

```
Filesystem                Size      Used   Avail   Use%   Mounted on
/dev/xxx/oss_vg-opt_vol   53G      27G    24G     54%    /xxx
...
```

- c. Skontrolujte, či veľkosť zostávajúceho priestoru zálohy spĺňa požiadavky na súbor zálohy. V nasledujúcom texte sa predpokladá, že veľkosť záložného súboru je 5 GB.
- Ak je zostávajúci priestor zálohy väčší ako 5 GB, prejdite na 6.
 - Ak je zostávajúci priestor zálohy menší alebo rovný 5 GB, kontaktujte správcu, aby ukladací priestor rozšíril.

6. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

7. Vytvorte úlohu na zálohovanie PowerEcho.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up the Management Plane**.
- b. Na zobrazenej stránke vykonajte operácie podľa výzvy.
- c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task list** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
- Ak je úloha zálohovania úspešná, prejdite na 8.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

8. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, kontaktujte technickú podporu.

- Zobrazenie podrobností o úlohe

1. Prihláste sa do PowerEcho.


- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

2. Na PowerEcho vyberte **System > Task List** z hlavnej ponuky.

3. Kliknutím  získate **Location Info** o neúspešnej naplánovanej úlohe na zálohovanie PowerEcho a opravte poruchu na základe **Location Info**. Ak je porucha odstránená, prejdite na 4. V opačnom prípade kontaktujte technickú podporu.

4. Vytvorte úlohu na zálohovanie PowerEcho.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up the Management Plane**.

- b. Na zobrazenej stránke vykonajte operácie podľa výzvy.

- c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.

- Ak je úloha zálohovania úspešná, prejdite na 5.
- Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmlu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-101217 Zlyhanie plánovaného zálohovania aplikácie produktu

Popis alarmu

Ak naplánovaná úloha na zálohovanie aplikácií produktu zlyhá, PowerEcho ohlásí alarm „Product Application Scheduled Backup Failure“. Tento alarm sa automaticky vymaže, keď sa úloha zálohovania úspešne vykoná.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101217	Kritické	Stav zálohy

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Alias produktu	Alias produktu.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.

Vplyv na systém

Naplánovaná úloha na zálohovanie aplikácií produktu sa nepodarí vykonať a bude ovplyvnená obnova údajov.

Možné príčiny

- Parametre zálohovania nie sú nakonfigurované.
- Záložné údaje sa nepodarilo uložiť na záložný server.
- Aplikáciu produktu sa nepodarilo zálohovať.

Postup

Vyberte zodpovedajúci postup odstraňovania problémov v tabuľke 1 na základe príčiny zlyhania zálohovania.


Tabuľka 1 Postup pri odstraňovaní zlyhaní zálohovania

Príčina	Postup
Parametre zálohovania nie sú nakonfigurované.	Podrobnosti nájdete v časti „Nastavenie parametrov zálohovania“.
Záložné údaje sa nepodarilo uložiť na záložný server.	Podrobnosti nájdete v časti „Kontrola konektivity a úložného priestoru záložného servera“.
Aplikáciu produktu sa nepodarilo zálohovať.	Podrobnosti nájdete v časti „Zobrazenie podrobností o úlohe“.

- Nastavenie parametrov zálohovania

1. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

2. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**.

3. Na stránke **Configure Backup Parameters** vykonajte operácie podľa výzvy.

4. Vytvorte úlohu na zálohovanie príslušnej aplikácie produktu na základe podrobností o alarme.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Product Application**.

- b. Na stránke **Back Up Product Application** vykonajte požadované operácie.

- c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.

- Ak je úloha zálohovania úspešná, prejdite na 5.
- Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.

- Ak alarm pretrváva, kontaktujte technickú podporu.
- Kontrola konektivity a úložného priestoru záložného servera
 1. Použijete PuTTY na prihlásenie do ľubovoľného databázového uzla PowerEcho ako používateľ **sopuser** v režime SSH.
 2. Ak chcete prepnúť na používateľa **ossadm**, spustíte nasledujúci príkaz:
> **su - ossadm**

```
Password: password for the ossadm user
```


3. Spustíte nasledujúci príkaz na kontrolu konektivity medzi databázovým uzlom a záložným serverom:

```
sftp backup server username@[IP address of the backup server]
```

```
Backup server username@IP address of the backup server's password:
```

- Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Prejdite na 4 .

```
Connected to IP address of the backup server
sftp>
```

- Ak sa zobrazia informácie podobné nasledujúcim, autentifikácia odtlačkom prsta medzi uzlom databázy a záložným serverom sa stratí alebo nebola nakonfigurovaná. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**. V oblasti **Configure Backup Server Parameters** kliknutím  prekonfigurujte odtlačok SFTP. Po úspešnej operácii prejdite na 4 . Ak operácia zlyhá, kontaktujte technickú podporu.

```
The authenticity of host '10.10.10.28 (10.10.10.28)' can't be
established.
```

```
...
```

```
No matching host key fingerprint found in DNS.
```

- Keď sa zobrazia nasledujúce informácie, stlačením klávesov **Ctrl + C** ukončíte zobrazovanie informácií o autentifikácii odtlačkom prsta SFTP. Ak sa vráti chyba časového limitu požiadavky, sieťové pripojenie je abnormálne. Skontrolujte a obnovte sieťové pripojenie. Po úspešnej operácii prejdite na 4. V opačnom prípade kontaktujte technickú podporu.

```
Are you sure you want to continue connecting (yes/no)?
```

4. Použijete PuTTY na prihlásenie na záložný server ako používateľ záložného servera v režime SSH.

NOTE

- Používateľ na prihlásenie na záložný server musí mať povolenie SSH. V opačnom prípade kontaktujte správcu servera, aby používateľovi pridelil povolenie.
- Ak sa riadiaci uzol používa ako záložný server, prihláste sa na záložný server ako používateľ **sopuser** v režime SFTP a potom prepnite na používateľa záložného servera.

- Ak je prihlásenie úspešné, heslo sa nezmení a záložný server funguje správne. Prejdite na 5.

- Ak prihlásenie zlyhalo, možnou príčinou je zmena hesla, vypršala platnosť hesla alebo je chybný záložný server. Kontaktujte personál O&M.

5. Skontrolujte miesto na záložnom serveri.


- Spustíte nasledujúci príkaz, aby ste skontrolovali dostupné miesto na záložnom serveri:
> **df -Ph**
- Zobrazia sa informácie podobné nasledujúcim. Skontrolujte hodnotu **Avail** v stĺpci **Mounted on** riadku, ktorý obsahuje oddiel zdieľaného adresára SFTP na záložnom serveri.

```
Filesystem                Size  Used Avail Use% Mounted on
/dev/xxx/oss_vg-opt_vol    53G   27G   24G   54% /xxx
...
```

- Skontrolujte, či veľkosť zostávajúceho priestoru zálohy spĺňa požiadavky na súbor zálohy. V nasledujúcom texte sa predpokladá, že veľkosť záložného súboru je 5 GB.
 - Ak je zostávajúci priestor zálohy väčší ako 5 GB, prejdite na 6.
 - Ak je zostávajúci priestor zálohy menší alebo rovný 5 GB, kontaktujte správcu, aby ukladací priestor rozšíril.

6. Prihláste sa do PowerEcho.

- Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

7. Vytvorte úlohu na zálohovanie príslušnej aplikácie produktu na základe podrobností o alarme.

- Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Product Application**.
- Na stránke **Back Up Product Application** vykonajte požadované operácie.
- Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
 - Ak je úloha zálohovania úspešná, prejdite na 8.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

8. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.
- Zobrazenie podrobností o úlohe
 1. Prihláste sa do PowerEcho.
 - a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Na PowerEcho vyberte **System > Task List** z hlavnej ponuky.
 3. Kliknutím > získate **Location info** o neúspešnej naplánovanej úlohe na zálohovanie aplikácií produktu a opravte poruchu na základe **Location Info**. Ak je porucha odstránená, prejdite na 4. V opačnom prípade kontaktujte technickú podporu.
 4. Vytvorte úlohu na zálohovanie príslušnej aplikácie produktu na základe podrobností o alarme.
 - a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Product Application**.
 - b. Na stránke **Back Up Product Application** vykonajte požadované operácie.
 - c. Z hlavnej ponuky vyberte **System > Task List** . Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
 - Ak je úloha zálohovania úspešná, prejdite na 5.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.
 5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže

ALM-101218 Zlyhanie plánovaného zálohovania databázovej aplikácie

Popis alarmu

Ak naplánovaná úloha na zálohovanie databázových aplikácií zlyhá, PowerEcho ohlásí alarm „Database Application Scheduled Backup Failure“. Tento alarm sa automaticky vymaže, keď sa úloha zálohovania úspešne vykoná.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101218	Kritické	Stav zálohy

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Alias produktu	Alias produktu.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.

Vplyv na systém

Naplánovaná úloha na zálohovanie databázových aplikácií sa nepodarí vykonať a bude ovplyvnená obnova údajov.

Možné príčiny

- Parametre zálohovania nie sú nakonfigurované.
- Záložné údaje sa nepodarilo uložiť na záložný server.
- Databázovú aplikáciu produktu sa nepodarilo zálohovať.

Postup

Vyberte zodpovedajúci postup odstraňovania problémov v tabuľke 1 na základe príčiny zlyhania zálohovania.


Tabuľka 1 Postup pri odstraňovaní zlyhaní zálohovania

Príčina	Postup
Parametre zálohovania nie sú nakonfigurované.	Podrobnosti nájdete v „Nastavenie parametrov zálohovania“.
Záložné údaje sa nepodarilo uložiť na záložný server.	Podrobnosti nájdete v časti „Kontrola konektivity a úložného priestoru záložného servera“.
Databázovú aplikáciu produktu sa nepodarilo zálohovať.	Podrobnosti nájdete v časti „Zobrazenie podrobností o úlohe“.

- Nastavenie parametrov zálohovania

1. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

2. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**.

3. Na stránke **Configure Backup Parameters** vykonajte operácie podľa výzvy.

4. Vytvorte úlohu na zálohovanie príslušnej databázovej aplikácie na základe podrobností o alarme.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Database Application**.

- b. Na stránke **Back Up Database Application** vykonajte operácie podľa výzvy.

- c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.

- Ak je úloha zálohovania úspešná, prejdite na 5.
- Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, kontaktujte technickú podporu.

- Kontrola konektivity a úložného priestoru záložného servera
 1. Použijete PuTTY na prihlásenie do ľubovoľného databázového uzla PowerEcho ako používateľ **sopuser** v režime SSH.

2. Ak chcete prepnúť na používateľa **ossadm**, spustíte nasledujúci príkaz:
> su - ossadm

```
Password: password for the ossadm user
```


3. Spustíte nasledujúci príkaz na kontrolu konektivity medzi databázovým uzlom a záložným serverom:

```
sftp backup server username@[IP address of the backup server]
```

```
Backup server username@IP address of the backup server's password:
```

- Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Prejdite na 4.

```
Connected to IP address of the backup server
sftp>
```

- Ak sa zobrazia informácie podobné nasledujúcim, autentifikácia odtlačkom prsta medzi uzlom databázy a záložným serverom sa stratí alebo nebola nakonfigurovaná. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**. V oblasti **Configure Backup Server Parameters** kliknutím  prekonfigurujte odtlačok SFTP. Po úspešnej operácii prejdite na 4. Ak operácia zlyhá, kontaktujte technickú podporu.

```
The authenticity of host '10.10.10.28 (10.10.10.28)' can't be
established.
...
No matching host key fingerprint found in DNS.
```

- Keď sa zobrazia nasledujúce informácie, stlačením klávesov **Ctrl + C** ukončíte zobrazovanie informácií o autentifikácii odtlačkom prsta SFTP. Ak sa vráti chyba časového limitu požiadavky, sieťové pripojenie je abnormálne. Skontrolujte a obnovte sieťové pripojenie. Po úspešnej operácii prejdite na 4. V opačnom prípade kontaktujte technickú podporu.

```
Are you sure you want to continue connecting (yes/no)?
```

4. Použijete PuTTY na prihlásenie na záložný server ako používateľ záložného servera v režime SSH.

NOTE

- Používateľ na prihlásenie na záložný server musí mať povolenie SSH. V opačnom prípade kontaktujte správcu servera, aby používateľovi pridelil povolenie.
- Ak sa riadiaci uzol používa ako záložný server, prihláste sa na záložný server ako používateľ **sopuser** v režime SFTP a potom prepnite na používateľa záložného servera.

- Ak je prihlásenie úspešné, heslo sa nezmení a záložný server funguje správne. Prejdite na 5.
- Ak prihlásenie zlyhalo, možnou príčinou je zmena hesla, vypršala platnosť hesla alebo je chybný záložný server. Kontaktujte personál O&M.

5. Skontrolujte miesto na záložnom serveri.

- a. Spustíte nasledujúci príkaz, aby ste skontrolovali dostupné miesto na záložnom serveri:

```
> df -Ph
```

- b. Zobrazia sa informácie podobné nasledujúcim. Skontrolujte hodnotu **Avail** v stĺpci **Mounted on** riadku, ktorý obsahuje oddiel zdieľaného adresára SFTP na záložnom serveri.

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/xxx/oss_vg-opt_vol	53G	27G	24G	54%	/xxx
...					

- c. Skontrolujte, či veľkosť zostávajúceho priestoru zálohy spĺňa požiadavky na súbor zálohy. V nasledujúcom texte sa predpokladá, že veľkosť záložného súboru je 5 GB.
- Ak je zostávajúci priestor zálohy väčší ako 5 GB, prejdite na 6.
 - Ak je zostávajúci priestor zálohy menší alebo rovný 5 GB, kontaktujte správcu, aby ukladací priestor rozšíril.

6. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.


NOTE

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

7. Vytvorte úlohu na zálohovanie príslušnej databázovej aplikácie na základe podrobností o alarme.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Database Application**.
- b. Na stránke **Back Up Database Application** vykonajte operácie podľa výzvy.
- c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
- Ak je úloha zálohovania úspešná, prejdite na 8.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

8. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.
 - Zobrazenie podrobností o úlohe
 1. Prihláste sa do PowerEcho.
 - a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.
-  **NOTE**

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero radiacích uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.
- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
 2. Na PowerEcho vyberte **System > Task List** z hlavnej ponuky.
 3. Kliknutím > získate **Location Info** o neúspešnej naplánovanej úlohe na zálohovanie databázových aplikácií a opravte poruchu na základe **Location Info**. Ak je porucha odstránená, prejdite na 4. V opačnom prípade kontaktujte technickú podporu.
 4. Vytvorte úlohu na zálohovanie príslušnej databázovej aplikácie na základe podrobností o alarme.
 - a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Database Application**.
 - b. Na stránke **Back Up Database Application** vykonajte operácie podľa výzvy.
 - c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
 - Ak je úloha zálohovania úspešná, prejdite na 5.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.
 5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.

ALM-101219 Plánované zlyhanie zálohovania operačného systému

Popis alarmu

Ak naplánovaná úloha na zálohovanie OS zlyhá, PowerEcho ohlásí alarm „OS Scheduled Backup Failure“. Tento alarm sa automaticky vymaže, keď sa úloha zálohovania úspešne vykoná.

Atribút alarmu

ID alarmu	Závažnosť alarmu	Typ alarmu
101219	Kritické	Stav zálohy

Parametre alarmu

Kategória	Parameter	Popis
Informácie o polohe	Alias produktu	Alias produktu.
	Názov siete	Názov lokality, pre ktorú sa generuje alarm.

Vplyv na systém

Plánovaná úloha zálohovania sa nevykoná a obnova údajov je ovplyvnená.

Možné príčiny

- Parametre zálohovania nie sú nakonfigurované.
- Nepodarilo sa uložiť údaje na záložný server.
- Zálohovanie operačného systému zlyhalo.

Postup

Vyberte zodpovedajúci postup odstraňovania problémov v tabuľke 1 na základe príčiny zlyhania zálohovania.


Tabuľka 1 Postup pri odstraňovaní zlyhaní zálohovania

Príčina	Postup
Parametre zálohovania nie sú nakonfigurované.	Podrobnosti nájdete v časti „Nastavenie parametrov zálohovania“.
Nepodarilo sa uložiť údaje na záložný server.	Podrobnosti nájdete v časti „Kontrola konektivity a úložného priestoru záložného servera“.
Zálohovanie operačného systému zlyhalo.	Podrobnosti nájdete v časti „Zobrazenie podrobností o úlohe“.

- Nastavenie parametrov zálohovania

1. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

2. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**.

3. Na stránke **Configure Backup Parameters** vykonajte operácie podľa výzvy.

4. Vytvorte úlohu na zálohovanie zodpovedajúceho operačného systému na základe podrobností o alarme.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Operating System**.

- b. Na stránke **Back Up Operating System** vykonajte operácie podľa výzvy.

- c. Z hlavnej ponuky vyberte **System > Task List** . Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.

- Ak je úloha zálohovania úspešná, prejdite na 5.
- Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, kontaktujte technickú podporu.

- Kontrola konektivity a úložného priestoru záložného servera

1. Použite PuTTY na prihlásenie do ľubovoľného databázového uzla PowerEcho ako používateľ **sopuser** v režime SSH.

2. Ak chcete prepnúť na používateľa **ossadm** , spustite nasledujúci príkaz:
> **su - ossadm**

```
Password: password for the ossadm user
```


3. Spustite nasledujúci príkaz na kontrolu konektivity medzi databázovým uzlom a záložným serverom:

```
sftp backup server username@[IP address of the backup server]
```

Backup server username@IP address of the backup server's password:

- Ak sa zobrazia informácie podobné nasledujúcim, sieťové pripojenie je normálne. Prejdite na 4.

```
Connected to IP address of the backup server
sftp>
```

- Ak sa zobrazia informácie podobné nasledujúcim, autentifikácia odtlačkom prsta medzi uzlom databázy a záložným serverom sa stratí alebo nebola nakonfigurovaná. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Configuration > Configure Backup Parameters**. V oblasti **Configure Backup Server Parameters** kliknutím  prekonfigurujte odtlačok SFTP. Po úspešnej operácii prejdite na 4. Ak operácia zlyhá, kontaktujte technickú podporu.

```
The authenticity of host '10.10.10.28 (10.10.10.28)' can't be
established.
...
No matching host key fingerprint found in DNS.
```

- Keď sa zobrazia nasledujúce informácie, stlačením klávesov **Ctrl + C** ukončíte zobrazovanie informácií o autentifikácii odtlačkom prsta SFTP. Ak sa vráti chyba časového limitu požiadavky, sieťové pripojenie je abnormálne. Skontrolujte a obnovte sieťové pripojenie. Po úspešnej operácii prejdite na 4. V opačnom prípade kontaktujte technickú podporu.

```
Are you sure you want to continue connecting (yes/no)?
```

4. Použite PuTTY na prihlásenie na záložný server ako používateľ záložného servera v režime SSH.

NOTE

- Používateľ na prihlásenie na záložný server musí mať povolenie SSH. V opačnom prípade kontaktujte správcu servera, aby používateľovi pridelil povolenie.
- Ak sa riadiaci uzol používa ako záložný server, prihláste sa na záložný server ako používateľ **sopuser** v režime SFTP a potom prepnite na používateľa záložného servera.

- Ak je prihlásenie úspešné, heslo sa nezmení a záložný server funguje správne. Prejdite na 5.
- Ak prihlásenie zlyhalo, možnou príčinou je zmena hesla, vypršala platnosť hesla alebo je chybný záložný server. Kontaktujte personál O&M.

5. Skontrolujte miesto na záložnom serveri.
 - a. Spustíte nasledujúci príkaz, aby ste skontrolovali dostupné miesto na záložnom serveri:
> **df -Ph**


- b. Zobrazia sa informácie podobné nasledujúcim. Skontrolujte hodnotu **Avail** v stĺpci **Mounted on** riadku, ktorý obsahuje oddiel zdieľaného adresára SFTP na záložnom serveri.

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/xxx/oss_vg-opt_vol	53G	27G	24G	54%	/xxx
...					

- c. Skontrolujte, či veľkosť zostávajúceho priestoru zálohy spĺňa požiadavky na súbor zálohy. V nasledujúcom texte sa predpokladá, že veľkosť záložného súboru je 5 GB.
- Ak je zostávajúci priestor zálohy väčší ako 5 GB, prejdite na 6.
 - Ak je zostávajúci priestor zálohy menší alebo rovný 5 GB, kontaktujte správcu, aby ukladací priestor rozšíril.

6. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

 **NOTE**

Ak je PowerEcho nasadené v režime klastra, to znamená, že existuje viacero radiacích uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.

7. Vytvorte úlohu na zálohovanie zodpovedajúceho operačného systému na základe podrobností o alarme.

- a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Operating System**.
- b. Na stránke **Back Up Operating System** vykonajte operácie podľa výzvy.
- c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
- Ak je úloha zálohovania úspešná, prejdite na 8.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.

8. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.

- Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
- Ak alarm pretrváva, kontaktujte technickú podporu.


- Zobrazenie podrobností o úlohe

1. Prihláste sa do PowerEcho.

- a. Prístup k PowerEcho získate na **https://client IP address of the PowerEcho:31945**.

NOTE

Ak je PowerEcho nasadené v režime klastra , to znamená, že existuje viacero riadiacich uzlov, prihláste sa pomocou jeho pohyblivej adresy IP.

- b. Na prihlasovacej stránke zadajte používateľské meno a heslo a kliknite na tlačidlo **Log In**.
2. Na PowerEcho vyberte **System > Task List** z hlavnej ponuky.
3. Kliknutím  získate **Location Info** o zlyhanej naplánovanej úlohe na zálohovanie operačného systému a opravte poruchu na základe **Location Info**. Ak je porucha odstránená, prejdite na 4. V opačnom prípade kontaktujte technickú podporu.
4. Vytvorte úlohu na zálohovanie zodpovedajúceho operačného systému na základe podrobností o alarme.
 - a. Na PowerEcho vyberte z hlavnej ponuky **Backup and Restore > Data Backup > Back Up Operating System**.
 - b. Na stránke **Back Up Operating System** vykonajte operácie podľa výzvy.
 - c. Z hlavnej ponuky vyberte **System > Task List**. Na stránke **Task List** skontrolujte, či bola úloha zálohovania úspešne vykonaná.
 - Ak je úloha zálohovania úspešná, prejdite na 5.
 - Ak úloha zálohovania zlyhá, kontaktujte technickú podporu.
5. Po úspešnom vykonaní úlohy zálohovania skontrolujte, či je alarm vymazaný.
 - Ak je alarm vymazaný, nie sú potrebné žiadne ďalšie kroky.
 - Ak alarm pretrváva, kontaktujte technickú podporu.

Vymazanie alarmu

ADAC: Po odstránení poruchy sa tento alarm automaticky vymaže.