The reasons for Data Center crash

Data operators sometimes make mistakes that can lead to the data center being stopped. However, most of these incidents can be avoided through maintenance measures, testing procedures and by the feeling and experience of system operators.

Data operators sometimes make mistakes that can lead to the data center being stopped.However, most of these incidents can be avoided through maintenance measures, testing procedures and by the feeling and experience of the system operators themselves.

A "data center with unintended power outages" is a polite way to talk about a malfunctioning data center leading to a shutdown.Even if the root cause is rooted in hardware errors, software bugs or human errors, most of these errors are possible, and should be prevented in advance.With the high level of risk redundancy applied in today's data centers, prevention of incidents is feasible.

Interestingly, minor errors can still happen all the time in a data center, and the damage caused by data centers stops working is not small, even in just one. minute.According to a Data Center Knowledge study, data center shutdowns can cost businesses around $ 7,900 a minute.In fact, 93% of companies have data centers with downtime for 10 days or more that go bankrupt within a year and 40% collapse immediately.And another study on 41 assessed data centers showed the average loss of unplanned outages including more than $ 179,000 in business disruptions, about $ 118,000 in sales. lost revenue and about 42 thousand dollars in productivity.If data center managers simply focus more on researching and overcoming the main causes of common errors, they will significantly reduce the potential risks.

The problem is that many data center operators and operators often focus only on growth, revenue instead of maintaining and strengthening what is already available.If you pay attention to administrators in many public and private data centers today, you will find that they are mostly interested in how to increase storage capacity, increase server density, and retrofit outdated server clusters into more modern facilities with a more efficient cooling system.Although all of this is great, essential and shows incredible growth in the data storage industry, it also shows why the phenomenon of data centers is in trouble. more and more common.

In this article, we will explore the common reasons that data centers are disabled, and raise what administrators can do to reduce or even eliminate them. completely these problems, as well as improving the stability of your system.

The reasons for Data Center crash

1. Human error
    1. System authorization is not correct
    2. Poor backup procedures
    3. Make too many changes
    4. Loose in HR management
2. System error
    1. Backup power is not guaranteed, equipment is old or misconfigured.
    2. Malfunction in the cooling system
    3. The automatic conversion process is not functional
    4. Outdated hardware
    5. Fire-fighting system has problems with water leakage
    6. Emergency power off is triggered at random
    7. Network attack, ddos
    8. Natural disaster
3. Steps to limit the damage caused by data center 'collapse'

Human error

These are the simplest causes and also one of the most unavoidable.Simply put, everyone can make mistakes.With 22% of outages resulting from human error, this cause is worth considering carefully and it is important that these errors can be prevented relatively easily.

System authorization is not correct

In fact, there are very few administrators who have full and unlimited access to all systems in the data center.Instead of granting this right to more people, access must be strictly managed.Otherwise, a serious error on the system is possible.In the case of Joyent in 2014, an experienced administrator unintentionally restarted all virtual machines in the company's eastern data center with just a few clicks.

Poor backup procedures

When planning maintenance tasks, an important but often the most forgotten step is the backup process.Often, processes are recorded but are not carefully considered and sometimes people do not completely revert everything to their original form after maintenance.

Make too many changes

During maintenance, if an administrator tries to make too many changes at the same time, this may cause some problems.First, administrators are often in a hurry because they have to complete a large number of tasks in a short period of time, which often leads to mistakes.Second, because a lot of changes are happening in the same time frame, it makes the post-troubleshooting problems change to become a much more difficult task.

Loose in HR management

It sounds a bit harsh, but employees need to know how to comply with the rules in the center and be severely disciplined when they commit violations.For example, no data center that allows employees to eat while working or an emergency switch must be clearly labeled and protected.These things seem small but can lead to major incidents, so make sure the rules are always strictly followed.

System error

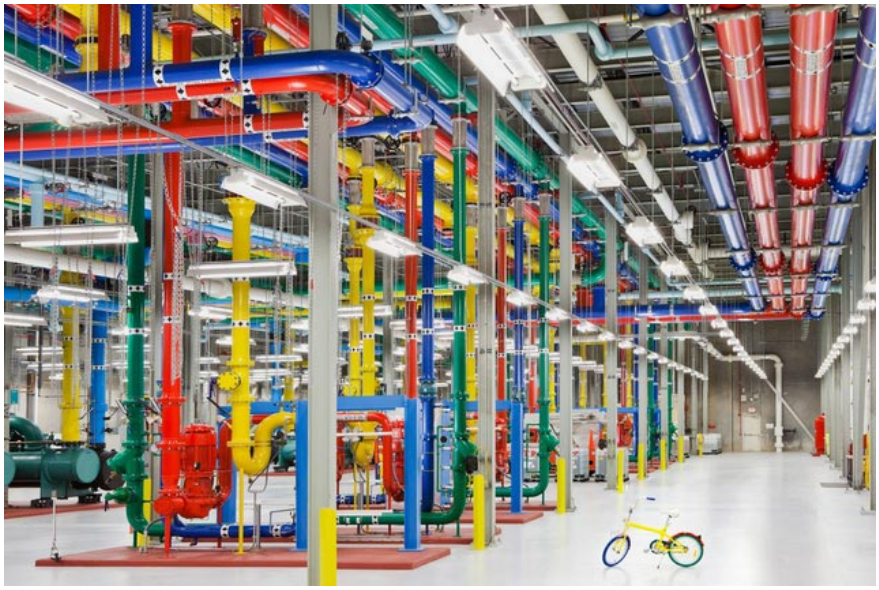
Backup power is not guaranteed, equipment is old or misconfigured.

The most common reason for a data center to stop working is due to a power outage.Power outages can happen all the time.Therefore, data centers are designed with redundant power sources in case the main source is switched off.Batteries or generator systems are often used as backup sources.The problem is, the battery may not be replaced promptly, the generator is not tested, maintenance leads to malfunction when a power failure occurs.All of this means your backup capabilities may not be available when you need them most.

In the event of a power outage, the UPS system uses batteries as backup power, making them an essential part of maintaining the uptime for data centers.However, batteries do not always work well.Maintenance is recommended by the manufacturer itself to check the battery status.At least quarterly, batteries must be checked for installation, discharge and charging properly.This includes visual inspection, capacity testing and regular monitoring through software or the UPS provider itself.

Also high temperature can shorten the battery life of the system.Building a dedicated UPS room can help reduce battery life wear.You should also avoid frequent battery discharge and good control of loose connections or worn connectors.In short, UPS is an especially important system, it requires reasonable design, proper use and strict maintenance.

Malfunction in the cooling system



Machinery systems in a data center consume a lot of electricity, meaning they emit a huge amount of heat during operation.A data center can become a crematorium after a minute of operation.That's why the cooling system plays an important role.And even if you have read temperature sensors and alerts sent to the administrator, you have to make sure that you have enough time to perform the center's backup cooling procedures before everything is broken. run'.

In addition, many cooling systems are not really designed to keep up with the increased heat levels in a large, modern data center.Again, outlining the circumstances in which your data center operates with 100% capacity can help plan for better cooling systems in the future.Setting up systems to warn system instabilities is also essential.You can use some thermal modeling software and some DCIM systems.In addition, chemical refrigerants are a better option than water-based systems.

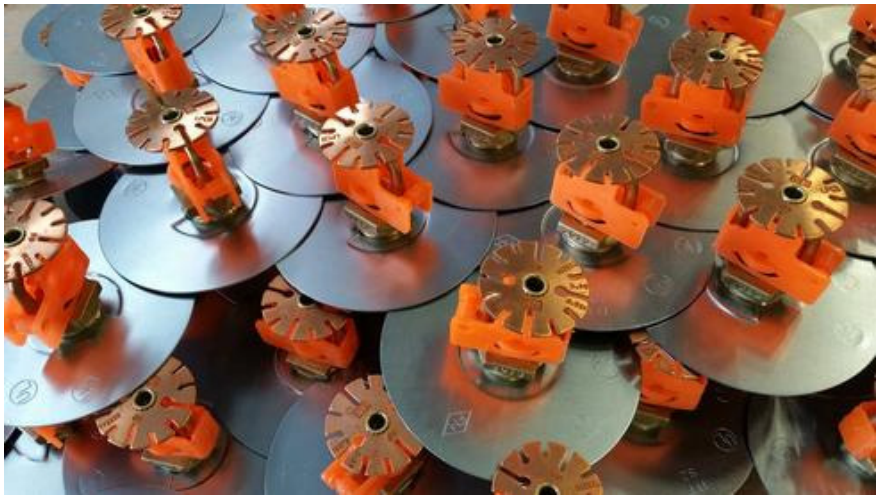
The automatic conversion process is not functional

Most service providers and organizations have backup data centers for production data centers.In the event of a power failure in the main data center, the backup data center will be automatically started and all traffic will be transferred to that backup.If done properly, the process must be seamless to the end user.Unfortunately, automatic failover often doesn't work as expected.The usual cause for this incident is the lack of regular checks.Even small changes in production infrastructure can have a major impact on the automatic failover process.Therefore, when making any changes to the infrastructure, automatic failover procedures will have to be checked to make sure nothing goes off the process.

Outdated hardware

All hardware of each system has a certain lifespan.And the longer you use a piece of hardware, the more likely you are to encounter a problem.Everyone knows this, but the case of an important application is malfunctioning just because it's running on 10-year-old hardware often happens.These problems often arise due to the lack of a comprehensive replacement and upgrade plan for the new hardware or software platform, or due to a lack of budget.If it's a money problem, you can't do anything more.But if you simply try to take advantage of it for as long as possible, the problem can happen at any time, and then, the damage caused by the incident can be even greater.

Fire-fighting system has problems with water leakage

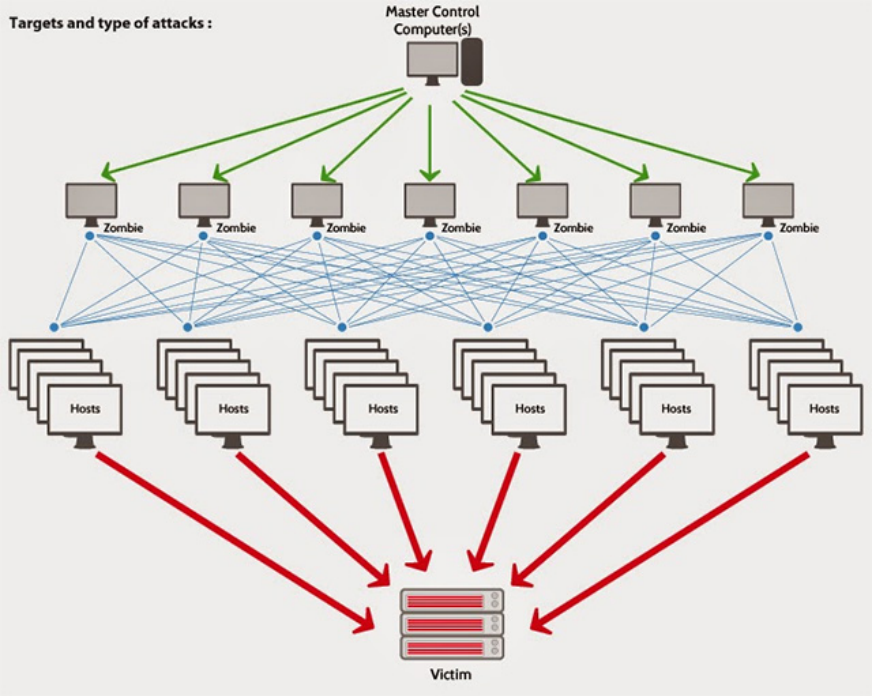


Most modern data centers use fireproof systems that do not use water so they do not damage the device if they are activated purposefully or accidentally.But many old facilities still use the traditional fire protection system in their data centers.Many cases of water leakage have caused major outages.

Emergency power off is triggered at random

The high level of physical security applied in most data centers is not simply about preventing thieves.They are also designed to avoid employees who don't understand how a data center works.For example, an application administrator enters the data center and accidentally activates an emergency power off (EPO).EPO is a big red button, which cuts off power to the entire system.And obviously, for those who do not understand, have no expertise, such confusion is entirely possible.

Network attack, ddos



In the past few years, cyber attacks have become one of the leading causes of data center "collapse", only from 2% in 2010 to 22% in 2016. Operators Data centers must act to establish systems to detect and minimize the risks of attack.

Data centers are hard to defend against a large-scale DDoS attack.Most ISPs provide some protection in layer 3 and layer 4 of the network, but your services need extra protection at layer 7, which can be specifically targeted via HTTP GET or sessions. Similar attack.Services that help mitigate damage such as firewalls, IPS / IDS and DDoS can be combined to reroute traffic.

Natural disaster

Rising storms and floods in the past time can cause significant paralysis for data centers.More than 250 natural disasters occurred in 2010 in the United States.According to statistics, the state of New Jersey, the United States suffered 63.9 billion dollars due to business interruption caused by super typhoon Sandy in 2012.

Steps to limit the damage caused by data center 'collapse'

If periodic maintenance stops are carefully planned and customers have been warned about the center's downtime, especially during a period of low traffic, customers will be more sympathetic and their losses will be significantly reduced.The big damage happens when it happens unexpectedly, and especially when it lasts, and there are additional problems.Keep the entire company's resource system stable so employees can perform their jobs effectively, reducing the burden on the IT department's shoulders.

Specifically:

1. Back up your data: In case you face an issue of deactivating the data center, your data (and more importantly your customer data) will be available when you catch Start troubleshooting and run again.Performing regular backups limits the risk of a real crisis.If your company is financially capable,

some products such as EMC's VPLEX product line or VEEAM's Backup and Replication software can help reduce incident time by automatically switching to the location. backup.

2. Maintain regular monitoring of the server system: Monitoring is a service you can perform regularly and usually does not cost too much.The 3rd party monitoring service will notify you of the risks when the server may stop working so you can handle the problem immediately.
3. Minimize human error: Be cautious when working or walking around a server or wiring system to prevent accidental damage or simply don't touch mysterious switches when you don't have a professional subject.Keep liquid away from mechanical systems.Call the data protection specialist anytime the server needs to upgrade or maintain, and comply with the rules of the center.

Each data center, from small centers to enterprise-scale facilities and service providers, must try to be 100% capable to provide reliable services to users.By taking the time to plan for the future, following the principles of maintenance, maintenance and human factors, your data center can avoid some of the most common causes leading to the problem stopped working.

see more

1. The largest data centers on the planet
2. Building data centers according to the cloud computing model
3. How to keep Facebook server from collapsing?
4. Explore inside Facebook's data center in Europe