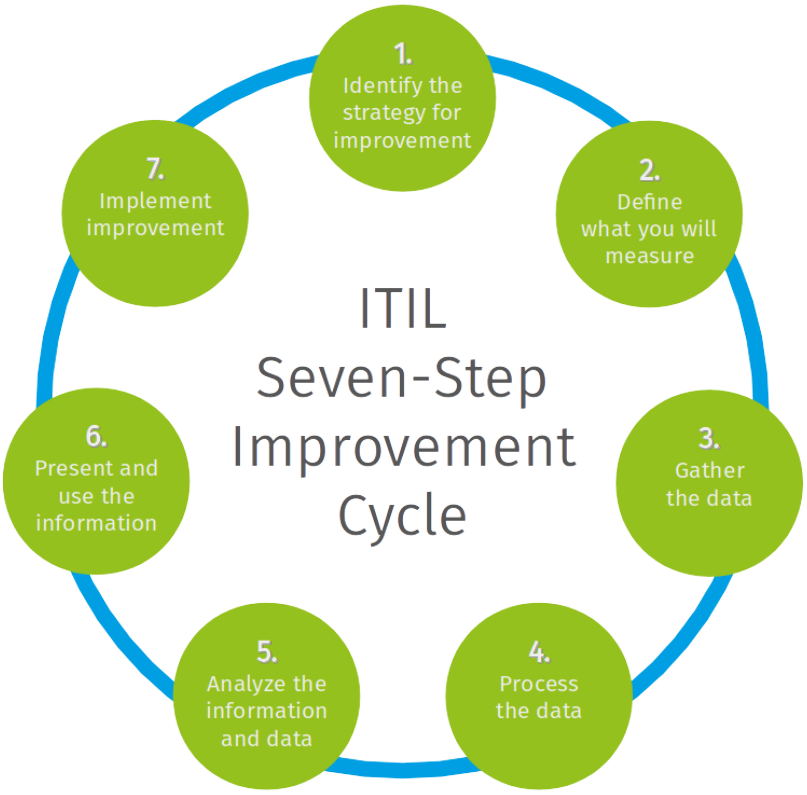
Knowledge River Data Center Optimization Services

How to increase Data Center Stability based on ITIL CSI?



Author : Jens Wissenbach and Sven Bittlingmayer
Last update : 30 Aug-2018

Table of Contents

1 Introduction

1.1 KnowledgeRiver GmbH, Germany

KnowledgeRiver > www.KnowledgeRiver.com is an independent partner for Data Center IT Service Providers with highest demands regarding cost-efficiency, reliability and performance. Our experience helps to continually improve the IT services.

The subject area 'Data Center Configuration Management (DCCM)' covers the entire 'Seven-Step Improvement Cycle' defined in ITIL.

Core is a market-unique analysis system for 'Data Center Systematical Analytics (DCSA)'.

All device classes - server, network, storage and virtualization layers - of almost all vendors are included. This assures that the overall configuration and the architectural IT design meets best practices and interoperability requirements.

The benefits are very numerous, but all of them are dominated by cost savings based on increased data center stability.

An overview about our service portfolio can be found here > www.KnowledgeRiver.com/services.

1.2 ITIL (IT Infrastructure Library)

In its current version - known as ITIL 2011 - ITIL is published as a series of five core volumes. Each of them covers a different ITSM (IT Service Management) lifecycle stage. Although ITIL underpins ISO/IEC 20000 (previously BS 15000) - the International Service Management Standard for ITSM - there are some differences between the ISO 20000 standard and the ITIL framework.

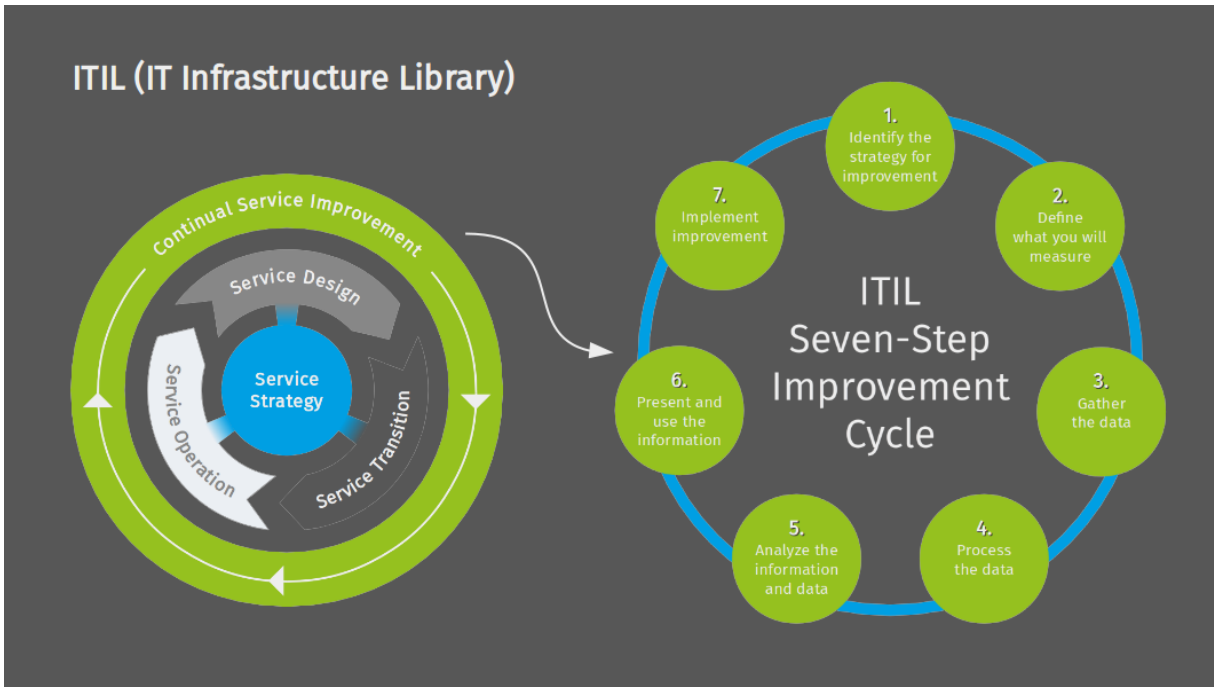
ITIL describes processes, procedures, tasks, and checklists which are not organization-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

Since July 2013, ITIL has been owned by AXELOS, a joint venture between Capita and the Cabinet Office. AXELOS licenses organizations to use the ITIL intellectual property, accredits licensed examination institutes, and manages updates to the framework. Organizations that wish to implement ITIL internally do not require this license.

ITIL 2007 - published in May 2007 - has **5 volumes/stages**. It was updated in July 2011 as ITIL 2011 for consistency. ITIL 2011 has **37 main processes**.

For an undisrupted operation of IT Services the stage **Continual Service Improvement (CSI)** is the most important.

Within CSI the so called **Seven-Step Improvement Cycle** is defined.



So, the biggest question for IT Service Providers is: **How can I make it work for me?**

ITIL References:
https://en.wikipedia.org/wiki/ITIL
https://www.axelos.com/best-practice-solutions/itil
https://wiki.en.it-processmaps.com

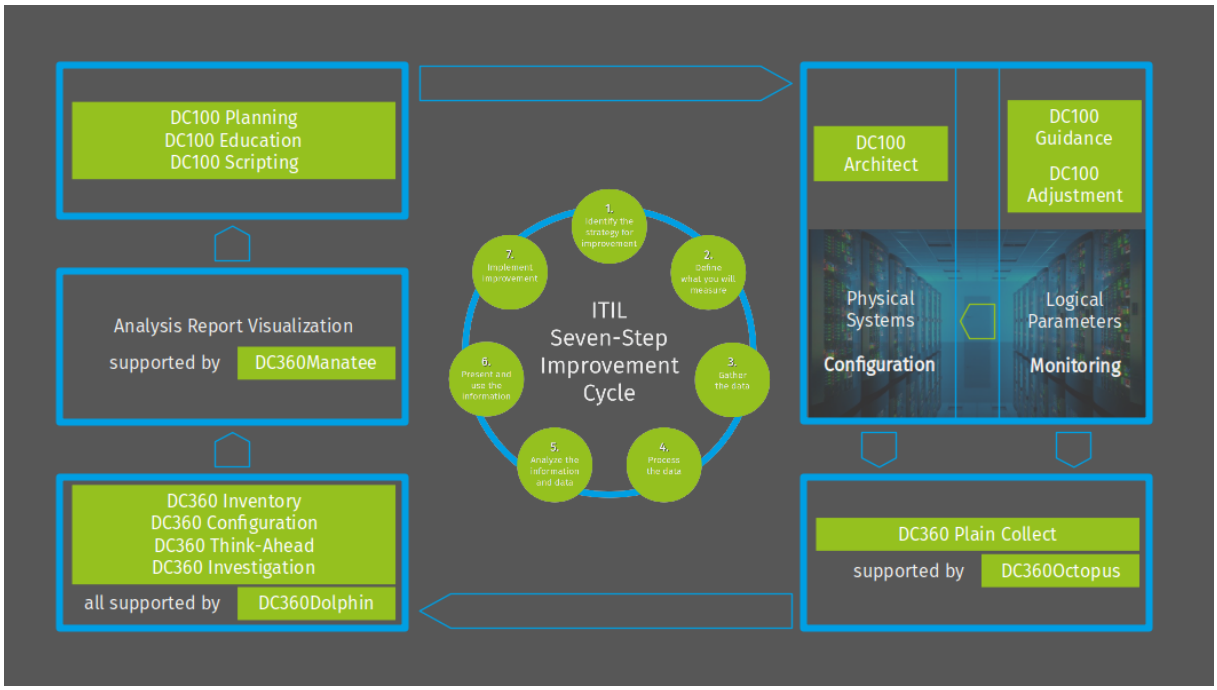
1.3 White Paper Information

This White Paper is based on a series of articles published by **Jens Wissenbach**.
He is one of the most experiences Data Center trouble shooters world-wide.

Here are the topics:

Why should I implement the ITIL CSI Seven Step Improvement Cycle?
How often should I run the ITIL CSI Seven Step Improvement Cycle?
What type of data do I have to collect during the ITIL CSI Seven-Step Improvement Cycle?
How do I have to prepare my environment for the ITIL CSI Seven-Step Improvement Cycle?
What is the order of probes during the ITIL CSI Seven-Step Improvement Cycle?
How do I read the report generated during the ITIL CSI Seven-Step Improvement Cycle?

2 What are the steps in the ITIL CSI Seven Step Improvement Cycle?



2.1 Identify the strategy of improvement

In this step the architecture of the services and their implementation are looked at. Standard questions are: Do you have a High Availability, dual Active Production Data Center design? Is there a separate Disaster Recovery site available? Is Production and Test/Development separated in isolated sites? Is the RTO/RPO for each service defined and tested? There are literally hundreds of these questions that go along with this step.

2.2 Define what you will measure

In this step guidance is needed to define the measurement points and adjustment of the warning and alert level in monitoring tools to tune these tools to the unique needs of the services.

2.3 Gather the data

The gathering of data is usually done when a problem has been seen in the environment, unfortunately usually only for single resources that are suspected to be the culprit but later on we realize that is was another component that we didn't suspected at the time. In order to have always all data from all resources the data collection process need to be automated and scheduled to allow a historically view into the environment.

2.4 Process the data

During this phase the unstructured data that has been collected in the step before need to be homogenized into structured data that can be handled by databases and data analysts.

2.5 Analyze the information and data

An intelligent tooling is needed to analyze the data in regards to interoperability, best practice and known problem pattern. It's actually a target-actual-comparison process.

2.6 Present and use the information

In this step the analysis need to be presented to the data center provider and his team. During the discussion of items in the prioritized list of findings the actions need to be defined that will be taken to eliminate the hardware errors, performance degradation issues, best practice implementation issues as well as interoperability issues.

2.7 Implement improvements

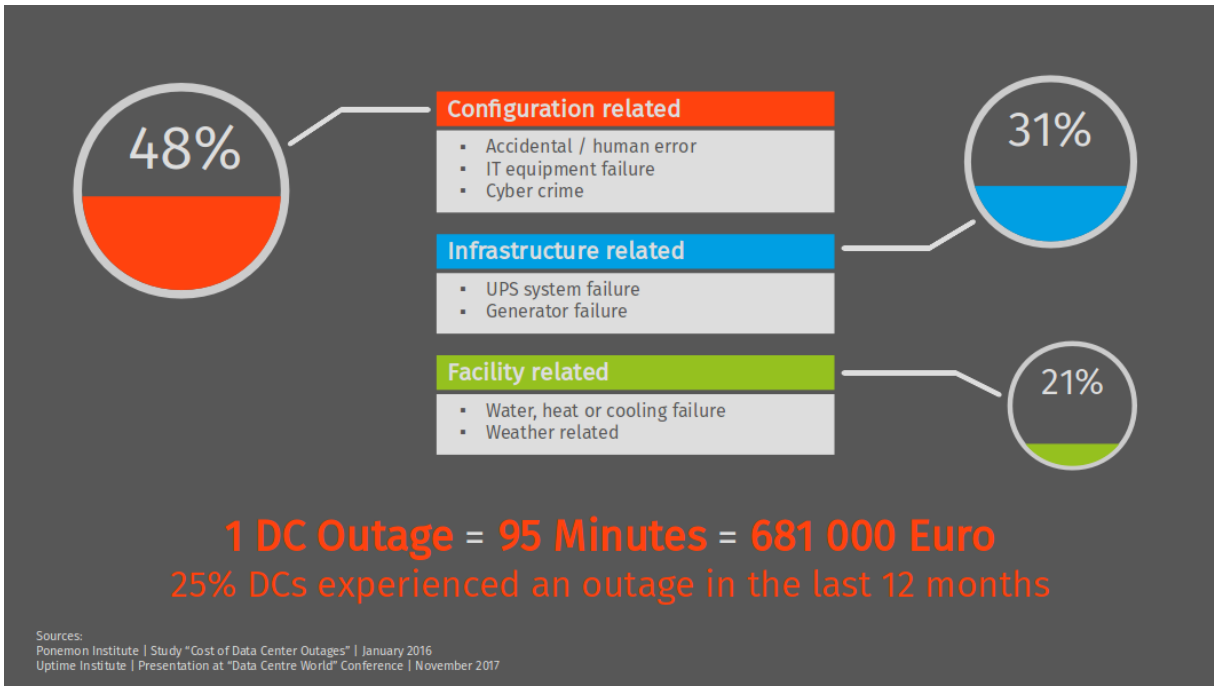
Together with the data center team the planning of the change requests need to take place. Scripting need to take place to speed up the implementation. Education need to take place to get a deeper understanding of the environment.

KnowledgeRiver is specialized to be your external help to get this process started in your organization.

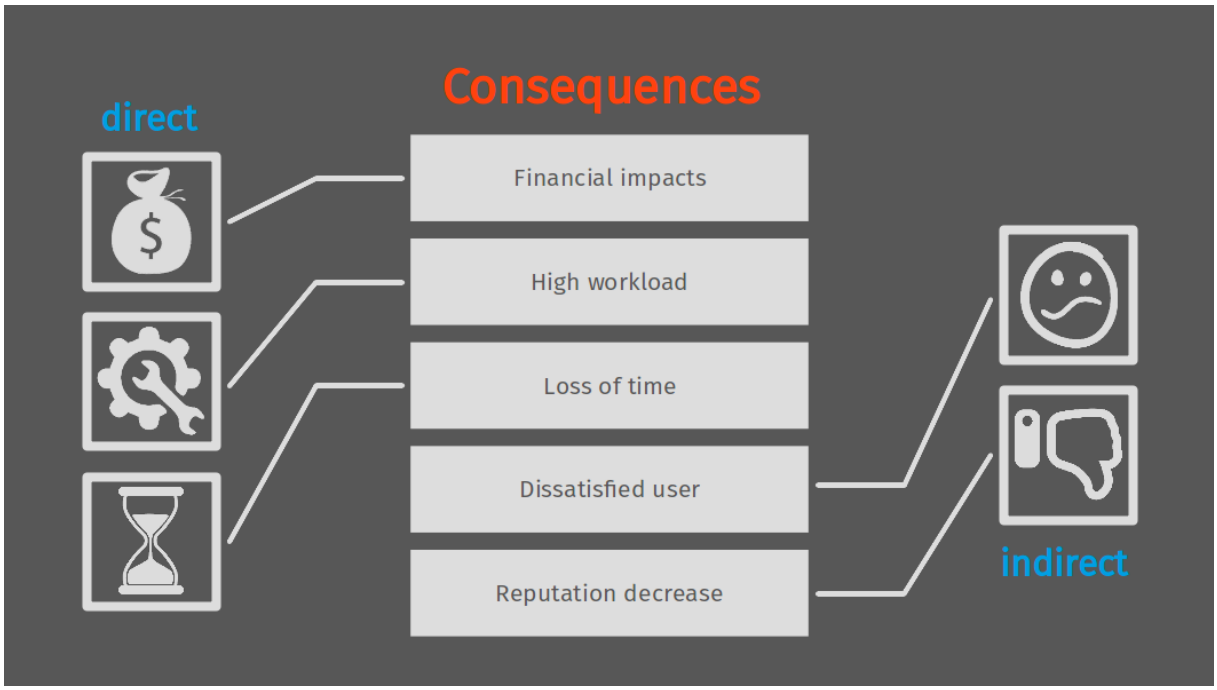
3 Why should I implement the ITIL CSI Seven Step Improvement Cycle?

The prevention rate of incidents is high in the 80% and the improved stability of the services is payback for the exercise.

This is one aspect of the need for the cycle.



Link to the source. Consequences of configuration related incidents:



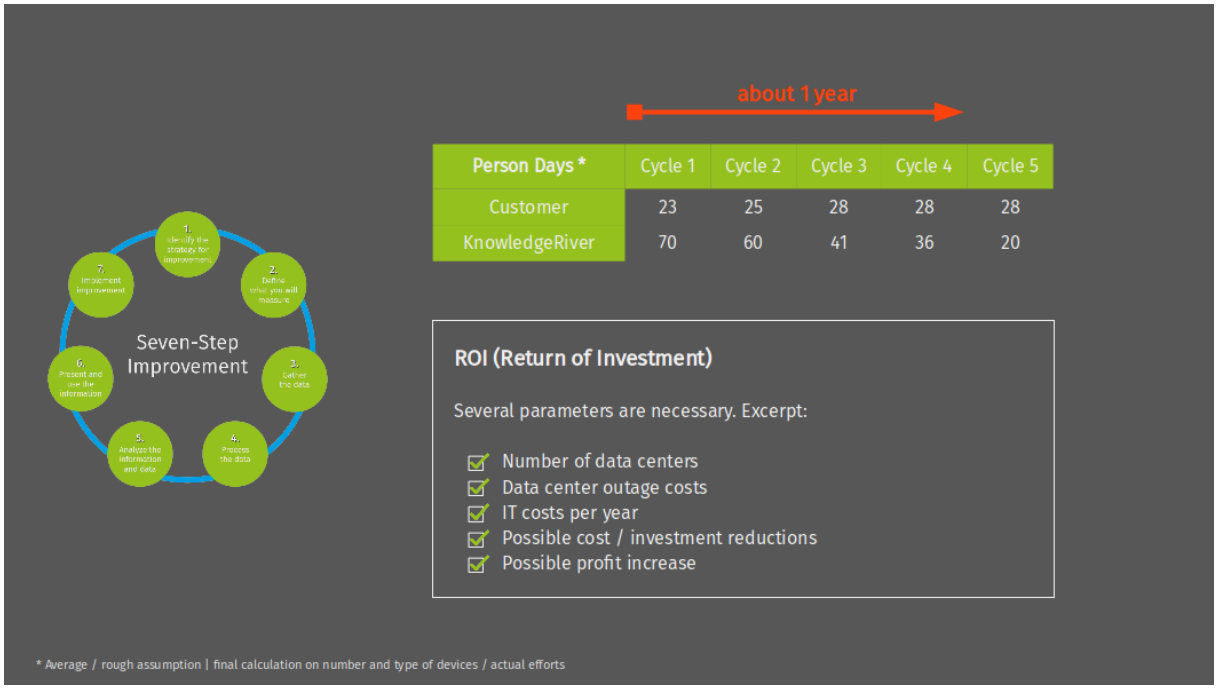
4 How often should I run the ITIL CSI Seven Step Improvement Cycle?

The frequency of the cycle highly depends on the stability and reliability of the data center environment.

An environment that runs with a small number of end-user and application owner complaints may need to walk through the cycle twice per year. The vendors of Storage, SAN, Network and Server devices provide PTF's (Program Temporary Fixes) normally twice a year to eliminate the know problems and make these fixes available for the wider community of customers. In order not to run into issues that other customers may have had in the passed 6 month, it is highly recommended to keep the microcodes of Storage, SAN, Network and Server devices up-to-date. Also changes can be added to the environment during these cycles and the stability and reliability of the environment is under constant monitoring.

If the environment experiences frequent abort or command timeout messages in the server, end-users and application owners complain about unpredictable runtime of batch jobs. The daily on-line respectively productive time gets shifted due to the fact that batch jobs didn't finish in time. This kind of problems indicate design, configuration, best practices, performance and/or hardware issues that need to be isolated and fixed. The recommendations for good running environments applies here as well. A frequency of four and more cycles per year may be needed to eliminate all issues.

Another reason to increase the frequency of cycles is any migration activity in the environment. Prior to a change it must be ensured that the environment is 'healthy and strong' enough to sustain a new more powerful resource. The past has shown that the environment became more unpredictable and unstable after new resources have been added to the data center. This is especially problematic for vendors of the new device, because they are the 'guilty guy' for any issue in the environment and they have to fight an 'uphill battle' against all the old issues.

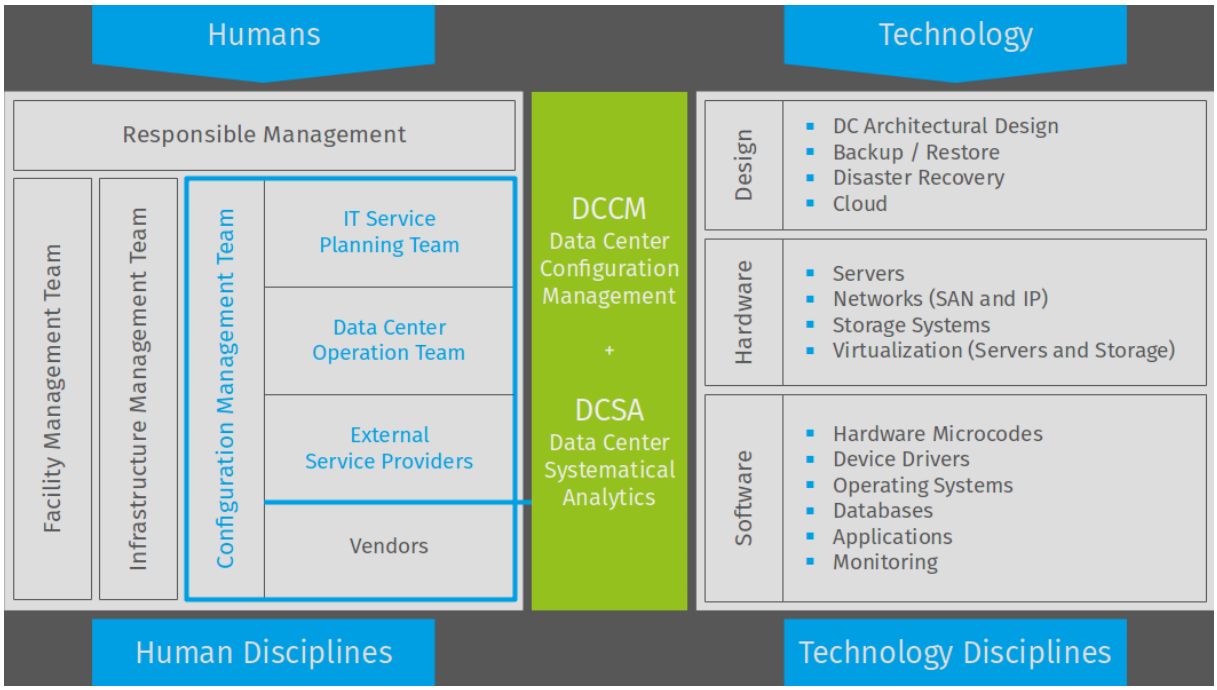


5 What type of data do I have to collect during the ITIL CSI Seven-Step Improvement Cycle?

The data that get collected during step 3 “Gather the data” depends on the resources you have in your data center. Normally these resources have vendor defined support data collection procedures. In most cases the procedures are Command-Line-Interface (CLI) commands that starts an internal device process to collect internal configuration and performance data including error logs. For some devices it is necessary to collect in addition CLI output information to reflect the relationship of the device to the overall environment. All these information are needed by the different vendors to analyze there hardware. Under no circumstances production data are collected during this step. The customer can review all data before sending them for analysis. The data package can be used for different tasks:

1. Stored for internal reference. Useful during implementation of changes to document the procedure.
2. Send to a vendor for analysis. It can happen, that this vendor is coming back with the message that he can not see any issue in his devices and that that the problem may lay in another device he is not responsible for. In this case, you have the data from these other devices already at hand. In many cases this situation can only be solved when the problem reoccurs several days or weeks later.
3. Send the data to someone who analyses the entire collection and is looking in addition for the root cause of an incident and upcoming issues... somebody who checks as well the environment against best practice guidelines and interoperability matrices.

Just the last case can speedup the process of analysis and is adding value to the collected data by providing more then 'just an analysis'. It also reduces the risk of potential future incidences.



6 How do I have to prepare my environment for the ITIL CSI Seven-Step Improvement Cycle?

6.1 Have all devices at a single time source

The logs on any device in the data center contain timestamps, this time stamp is based on the system clock of the device. If this clock has a different time zone or clock setting then the devices around it then it is nearly impossible to follow a problem from one device to another. In order to overcome this issue all devices need to follow a single device that provides a Network Time Protocol (NTP) synchronization service.

6.2 Have all system logs converged on a single server

The logs entries generated by a server can be send to a syslog-server within the environment. With the timestamps synchronized and the log entries of all Server, SAN, Virtualization and Storage devices in a single log it becomes easier to follow problems in the environment.

6.3 Have a centralized SFTP Server

The centralized SFTP server is needed to collect information from devices that can't be obtained via direct commands to the device. These are typically DS8000 PE-Packeges, Brocade support save outputs and a few other packages. The more important reason for having such a server is the distribution of microcodes. The centralized SFTP server allows a centralized management of the microcodes of all devices in the environment.

6.4 Have a centralized monitoring for all devices

The monitoring of devices is important to have a one minute interval performance statistics and error logging facility. There are many tools out there like the XORUX Stor2RRD/LPAR2RRD tools to long for storage and LPAR's information as well as Spectrum Control from IBM or EMC control center. The difference between these tools is like the difference between a VW Beetle and a Rolls-Royce, they are both cars but the style of transportation is different.

6.5 Have a naming convention that allows you to identify a resource by it's alias

The naming convention of an environment allows a identification of site, device, application and ID for each resource. These resources are WWPN's, Volumes, Nodes, Cluster, Storage subsystems, SAN Switch, Server and any other device that is within the

data center. The naming convention is defined in a document that all administrator have available to name new devices accordingly as soon as they get connected to the environment. This makes now each SNMP or error entry for the device easy to identify.

6.6 Have an automated configuration and support log gathering process

In order to have ALL information gathered during an incident it is important to automate the process as far as possible. The support logs of a system may wrap or the device that was under suspicion at the beginning of the issue is not the culprit. In these cases the surrounding devices may have information that can help to find the root cause for a problem. The KnowledgeRiver DC360Octopus is such a tool that allows the automation of Storage, SAN, Server and Virtualization layer support data collection. The collected data also allows a third party to have a look at the environment to provide recommendations that may help to prevent issues in the future.

6.7 Have a centralized Web-Server for administration

The centralized Web-Server allows the integration of tools like DC360Octopus, openDCIM, CACTI, ITop and others. The Knowledge Base functionality need to be included as well where the administrator can write down article that can be used within the data center to describe procedures and processes. All of these functions mentioned in this aricle are installed in the DC360Manatee virtual machine from KnowledgeRiver.

7 What is the order of probes during the ITIL CSI Seven-Step Improvement Cycle?

A data center is like a living organism, the nerves in this organism determine what it can and what it can't do. In order to become a healthy data center the communication paths between the different elements need to be stable, reliable and they need to perform. A data center has two layer of nerves, the Ethernet (IP) and the Fiber Channel (FC) layer. While the IP layer communicates with the outside world, the FC layer is responsible for the inner communication. The analysis and problem determination process need to start with the hardware error logs, then configuration and best practice implementation of the FC layer. The very first thing that need to be looked at is hardware errors. A healthy SAN (Storage Area Network) that is comprised out of FC elements should not have more then one hardware error per year per port. If we keep that ratio in mind then we should not see any Hardware error (CRC, Encoding, to long, or to short error) within a 6h window in a standard SAN of less then 2000 ports. The next issue that need to be looked at is congestion and the end form of a congestion the Discarded Class 3 error rates. There should be under no circumstance a discarded class 3 error at any time in the environment. The "Buffer to Buffer Zero" counts should not exceed 100000 in a 6h window. Other areas that need to be looked at is the buffer consumption on ISL (Inter-Switch Links), the bandwidth utilization and the congestion index of ports, the inter-site communication, etc.

After the SAN has been cleaned the next area that need to be sorted is the backend storage. The storage ports need to be looked at from the same prospective as the SAN ports but here especially from the inside of the storage subsystem. Errors on these ports get only be logged inside the storage subsystem. The best practice implementation of the subsystem need to be checked. Single resource over utilization, remote copy, easy tier configuration, tiering configuration, etc.

After these two items the Storage Virtualization layer need to be checked with all it's implementation regulations and error counter. Very much all the checks that have been done so far need to be repeated for this layer as well.

Now we come to the Server layer where we have the same counter as in a subsystem when it comes to SAN errors. The server have on top of this also error logs, CPU/Memory utilization issues etc. All of this applies to standard Server as well as the Server Virtualization layer.

Now the IP layer need to be checked and monitored to understand the performance impact of the IP network. The IP network is one of the last elements that need to be checked due to the fact that this layer can not perform if the layer below have issues.

Overall of these hardware related information the interoperability of all involved microcodes need to be checked and the end-to-end performance of the environment in a one minute interval. Every configuration mismatch can influence the performance of any

resource in the environment in an unpredictable way. Therefore a continues and highly automated monitoring and analysis need to be in place to keep all elements of a data center in balance.

The end-user will alway say **"My application is slow!!"**. But that is only a matter of perception. The problem may be somewhere in the stack of resources that he uses to perform his action. We need to make sure that everything runs at it's best possible stability, reliability and performance.

8 How do I read the report generated during the ITIL CSI Seven-Step Improvement Cycle?

The report generated in step **4. Process the data** and **5. Analyze the information and data** is a compressed file that can be downloaded from our homepage when you login and list your projects. This ZIP-file contains a directory structure that allows a user to navigate through the provided information.

The root directory is called CustomerReport. It contains two additional directories: Results and TechnicalDetails.

The Results directory contains the DC360Overview.html and several other files that are needed to drill down from this point into the results. This file contains at the top statistics like how many probes have been executed for which device type and the number of passed, warning and failed probes. It contains as well pie chart representations of the amount of issues found in each device type as well as a recommendation list for IT Service Provider with fundamental items that should be looked at every day in a data center. For example, are all resources running with NTP, are all SNMP messages handled and understood, is there a single speed in the SAN, and several more. This html also contains links to the prioritized list of findings. This list allows a issue elimination starting with the issue that harms the environment the most at this moment and goes down to the least impacting issue that may just be a best practices violation.

The TechnicalDetails directory contains a spreadsheet representation of all areas where problems are detected. These XLS files are referenced in the results section. It also contains a directory called AdditionalInformation; this contains all XLS files generated during the analysis and in addition a directory called CSV. The CSV directory contains all information in comma-separated value format. Therefore a data upload is possible straight into a database for additional analysis, if this is required.

9 Wrap-Up

KnowledgeRiver can help in any phase of the ITIL CLI Seven-Step Improvement Cycle.

Just get in contact with us:

KnowledgeRiver GmbH
Germany
contact@KnowledgeRiver.com
www.KnowledgeRiver.com