Datové zdroje a jejich popis					
Název	**Zdroj dat**	**Obsah a typ dat**	**Použití, očekávané výstupy**	**Poznámky a odkazy**	**Očekávané korelace a vazby**
Kerberos	logy Kerbera	počty přihlášení uživatelů k jednotlivým systémům (kdo, kdy, odkud, kam, přihlášen/odmítnut)	časový průběh počtu přihlášených podle systémů - anomálie mohou znamenat útok či poruchu		nagios
Síť	síťové logy	parametry provozu (zatížení vnitřních i vnějších linek), objemy přenesených dat	neobvyklé hodnoty parametrů jsou příznakem přetížení či poruchy		
Logy	serverové logy	chybové zprávy, textový formát s velkou variabilitou, obtížná normalizace	detekce abnormálních stavů ? Získáme něco víc než nagios ?		
Unix servery	vzorky ze serverů (atop a podobně)	numerické parametry zátěže (počty procesů, obsazená paměť, obsazení disku...)	neobvyklé hodnoty parametrů jsou příznakem přetížení či poruchy		nagios
Windows servery	vzorky pomocí sondy nagiosu	numerické parametry zátěže (počty procesů, obsazená paměť, obsazení disku...)	neobvyklé hodnoty parametrů jsou příznakem přetížení či poruchy	http://nagios.sourceforge.net/docs/3_0/monitoring-windows.html http://sourceforge.net/projects/nscplus/	nagios
web servery	logy apache	počty přístupů ze ZČU a z venku	struktura uživatelů jednotlivých webů podle pracovišť, časový průběh využívání aplikací - anomálie mohou znamenat útok či poruchu provozni parametry weboveho serveru	http://mathias-kettner.de/checkmk_livestatus.html	nagios, servery
file servery	logy AFS	počty přístupů k volumům, chyby replik, rozmístění serverů v lokalitách a toky dat mezi nimi			
Email	logy email serverů	počty připojených uživatelů, počty odeslaných, doručených mailů…	detekce abnormalit (neobvykle vysoký počet emailů při spamovém útoku, neobvykle nízký počet emailů při poruchovém stavu)		nagios
Učebny	logy IS stanic	využití stanic v učebnách (počty pracujících a volných strojů)	časový průběh využívání učeben, odhad volných míst v prostoru a čase, vytipování lokalit k posílení či redukci		
Incidenty	detekční systémy, bezp. skupina		možná poslouží jako ověření detekce incidentů z jiných zdrojů		
Nagios	sondy a logy nagiosu	Provozní stav systémů (označení systému nebo subsystému a jeho stav - funguje/nefunguje)	informace o poruchových stavech		servery, email, kerberos
Nagios	performance sondy	Provozní parametry systémů	sondy vraci (po instalaci performance sond) i provozní parametry	http://nagios.sourceforge.net/docs/1_0/perfdata.html	
Kalendář a akce	vlastní db	rozlišení času a vliv plánovaných událostí (den, noc, pracovní, víkend), semestr, zápočtové a zkouškové období, plánované odstávky, předzápis…	korelace dle času s ostatními zdroji, zvýšení zátěže může být generováno konkrétním typem akce vytvoření seznamu výjimečných dnů (svátky, volna, předzápis)		prakticky se vším, co má časový parametr
hosts	db saurona, evidence IS	upřesnění typu stroje, kategorie, místo kde je umístěn, přiřazení k pracovišti	statická informace, pouze rozšiřuje identifikaci stroje o další atributy		
users	IdM	kategorizace uživatelů (student, učitel, zaměstnanec...), přiřazení na pracoviště	statická informace, rozšiřuje identifikaci uživatele o další atributy (typ uživatele, příslušnost k pracovišti, přidělené systémy)		
AFS	IdM	obsazený/požadovaný prostor	diskové nároky v závislosti na projektu, pracovišti, uživateli		
Portál	logy	počty pracujících uživatelů, konkrétní aplikace			
Inis	?	počty pracujících uživatelů, konkrétní aplikace			
JIS	data přechodů stavů	datum vydání karty, kategorie uživatele, typ karty datum vrácení karty, důvod vrácení karty datum automatické blokace	anomálie v průběhu výdeje nebo vracení karet detekce vadných serií karet (nadměrné vracení z důvodu poškození) neobvykle vysoký počet automaticky blokovaných karet může znamenat poruchu v systémech		
JIS	logy sirius	záznam o použití karty na snímači	zvýšený výskyt odmítnutých karet nebo žádné záznamy - příznaky poruchy		
RT	požadavky	datum vzniku požadavku, fronta vzniku, fronta kudy prošel	neobvykle vysoký počet nových požadavků v některých frontách může signalizovat problém s provozem		
ORACLE DB	logy serveru	počty dotazů, vytížení databáze	anomálie v zatížení strojů -> porucha nebo kritický stav	http://www.remote-dba.net/t_tuning_stats$sysstat_table.htm http://www.oracle-base.com/articles/10g/AutomaticWorkloadRepository10g.php	