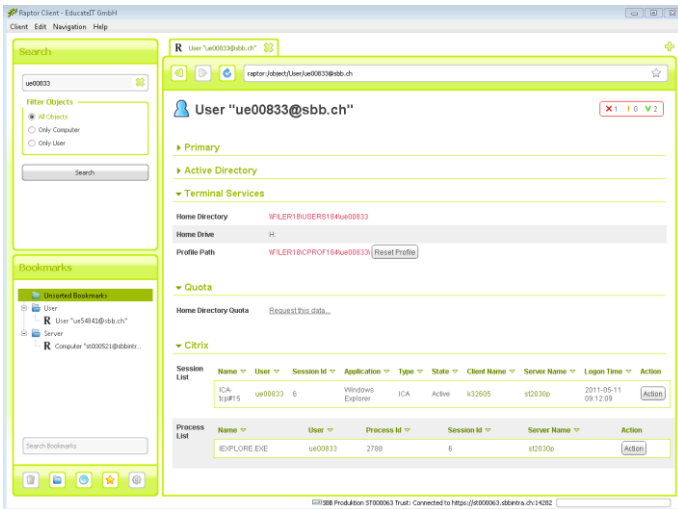


Raptor Service Desk Support System



Einsatzbereich

RAPTOR ist eine Software Lösung für den Service Desk in Terminal Server/Citrix Farmen und Fat-Client Umgebungen aller Grössen. RAPTOR optimiert die Erstlösungsrate im 1st und 2nd Level Support bei der Unterstützung der Benutzer durch den Service Desk.

Optimierte Oberfläche

RAPTOR wurde für die Nutzung durch 1st und 2nd Level Support-Mitarbeiter optimiert. Diese können mit minimalen Kenntnissen der technischen Systeme Störungen beseitigen und Routineaktionen, wie die Rücksetzung von Passwörtern, auslösen.

Kurze Reaktionszeit

Im Benutzersupport zählt für die Anwender eine kurze Reaktionszeit, d.h. die relevanten Informationen müssen für den Support-Mitarbeiter innerhalb von wenigen Sekunden verfügbar sein. RAPTOR wertet deshalb die wichtigsten Informationen der überwachten Server in Echtzeit aus und stellt diese unmittelbar zur Verfügung, damit der Kunde am Telefon nicht warten muss.

Optische Aufbereitung

Die Gliederung der Informationen spielt eine entscheidende Rolle. RAPTOR ruft weitergehende Informationen innerhalb weniger Sekunden direkt von den Zielsystemen ab und stellt sie in der gleichen Benutzeroberfläche dar. Sofern Informationen nicht unmittelbar angezeigt werden können, sieht der Anwender, welche Informationen im Hintergrund noch ermittelt werden.

Funktionen

Optimale Unterstützung des Service Desk durch

- intuitive Benutzeroberfläche
- rasches Auffinden der Benutzersitzung
- schnelle Anzeige der relevanten Eigenschaften
- Benutzerdefinierte Aktionen auf Objekte
- Remote Management der Benutzersitzung
- Unterstützung des Benutzers durch Remote Control (Shadowing) der Benutzersitzung
- Unterstützung bei der Problemanalyse durch Expertensystem
- Sicherheit durch rollenbasierte Berechtigungen und mandantenfähige Oberfläche

Erweiterbarkeit

RAPTOR ist skalierbar und bildet eine stabile und sichere Kommunikationsbasis.

Durch das modulare Konzept lässt sich RAPTOR flexibel erweitern und an firmenspezifische Prozesse und Anforderungen anpassen. Erweiterungen sind an Client, Server und Agent möglich.

Basierend auf den Kernfunktionen stehen Module für die Integration in Citrix, Active Directory und klassische Fat-Client Umgebungen zur Verfügung sowie kundenspezifische Module z.B. zur Anbindung an das Incident Management des Service Desk.

Citrix Modul

Das Citrix Modul erweitert die Informationen und Aktionen in RAPTOR zur Unterstützung der Benutzer in Citrix- und Terminal Server Umgebungen. Benutzersitzungen und laufende Prozesse auf den Terminal-Servern werden angezeigt und können durch den Service Desk beendet werden.

Active Directory Modul

Mit dem Active Directory Modul wird RAPTOR in folgendem Bereich stark erweitert:

Die Authentifizierung der Anwender erfolgt via Active Directory; so lassen sich auch Zugriffsrechte auf RAPTOR durch Active Directory Gruppen steuern.

Bei der Suche nach Computern und Benutzern kann Active Directory als Quelle verwendet werden, die gefundenen Objekte werden mit relevanten Informationen aus dem Microsoft Verzeichnis ergänzt.

Raptor Service Desk Support System

Systemarchitektur

RAPTOR besteht aus drei Komponenten:

- dem Client für den Service Desk Mitarbeiter
- dem Management Agent, der Daten auf den Zielsystemen sammelt
- dem Management Server, der die gesammelten Daten verwaltet

Der Client

Der Client bietet dem Anwender des Systems eine einfache Schnittstelle, mit der er alle für ihn relevanten Informationen schnell findet. Über diese Schnittstelle kann der Anwender nach verwalteten Objekten wie Servern, Clients und Benutzern im Netzwerk suchen. Zu jedem gefundenen Objekt erhält der Service Desk Mitarbeiter eine Übersicht alle relevanten Informationen. In dieser Oberfläche kann er technologie- oder unternehmensspezifische korrigierende Aktionen ausführen.

Der Management Server

Der Server speichert und analysiert die Informationen der überwachten Systeme und liefert diese Informationen an autorisierte Clients.

Der Raptor Agent

Der Agent arbeitet als Service auf den überwachten Servern. Er sammelt relevante Informationen wie zum Beispiel angemeldete Benutzer, Sitzungen und laufende Prozesse und sendet diese zur Analyse an den zentralen Server.

Leistung und Skalierbarkeit

RAPTOR wurde auf hohe Performance besonders in grossen Citrix-Umgebungen optimiert. Dabei spielt es keine Rolle, ob 10, 100 oder 1000 Server überwacht werden, durch die verteilte Logik entstehen keine Engpässe. Lediglich der zentrale Management Server muss entsprechend der Gesamtgrösse der Umgebung dimensioniert werden.

Expertensystem

Ein eingebautes Expertensystem erleichtert dem Support-Mitarbeiter den Überblick über die angezeigten Informationen. Es lassen sich Regeln definieren, die aus einzelnen Attributen oder einer Kombination verschiedener Attribute den angezeigten Betriebsstatus („Fehler“, „Warnung“ oder „störungsfreier Betrieb“) ermitteln.

Die Resultate dieses Regelwerks werden sortiert und farbig übersichtlich dargestellt und unterstützen den Support-Mitarbeiter bei der Erkennung und Bewertung von Fehlerzuständen.

Schutz der Informationen

Um die Informationen zu schützen, welche durch das RAPTOR System gewonnen werden, ist dieses in sich geschlossen.

Die Kommunikation zwischen dem Client und dem Management Server ist verschlüsselt. Dasselbe gilt für die Kommunikation zwischen den einzelnen Agenten und dem Server.

Ausfallsicherheit

Um die Ausfallsicherheit des Systems zu garantieren, kann der zentrale Management Server redundant betrieben werden. Dabei kennt jeder Agent auf den überwachten Servern eine Liste mit verfügbaren Management Servern. Fällt der primäre Management Server aus, wechseln alle Agenten automatisch auf den sekundären Server.

Dadurch kann die Ausfallzeit in einem solchen Fall minimiert werden. Je nach Konfiguration ist das gesamte System trotz Totalausfall des primären Servers beispielsweise innerhalb von wenigen Minuten wieder voll einsatzbereit.

Granulare Zugriffskontrolle

Der Zugriff auf Informationen und Aktionen kann bis auf eine sehr feine Ebene gesteuert werden. Dabei können Zugriffsregeln auf Gruppen und einzelne Anwender gesetzt werden.

Die gesamte Konfiguration der Zugriffsrechte wird zentral durch den Management Server verwaltet.