INFOSERVE SERVICE CARD PLATIN

INFOSERVE
>eurodata-Gruppe

BESTANDSAUFNAHME UND DOKUMENTATION:

Mit der Anlage Ihrer SERVICE CARD geht die entsprechende Dokumentation des zu betreuenden Systems einher, sodass unsere Service-Mitarbeiter im Support- und Beratungs-Fall über die zur Unterstützung erforderlichen Basisinformationen zu Ihrem System verfügen.

i Für die Erbringung der Service-Leistungen Support, Monitoring, Patchmanagement, Backup der Konfiguration und zentrales Logmanagement durch INFOSERVE müssen bestimmte technische Voraussetzungen* geschaffen werden.

SUPPORT:

Telefon zu den Geschäftszeiten

Telefon außerhalb der Geschäftszeiten

E-Mail

! Wenden Sie sich bitte in dringenden Fällen, insbesondere außerhalb der Geschäftszeiten, grundsätzlich telefonisch an uns.

MONITORING:

1. **Check VM (hostcheck/ping)**
2. **Check externer Service**
3. **Checks Systemzustand – Standard-Umfang (Disk, Load)**
4. **Weitere Checks auf Kundenwunsch**

i Die genannten Punkte 1-3 sind durch die SERVICE CARD abgedeckt, es gelten jedoch die u. g. technischen Voraussetzungen*. Die technischen Voraussetzungen für die Punkte 1-3 gelten auch für Punkt 4. Falls realisierbar, entstehen durch die damit verbundenen Aufwände evtl. zusätzliche Kosten. Weitere Informationen sind dem Datenblatt Monitoring zu entnehmen – *siehe Anlage Datenblatt Monitoring.*

PATCHMANAGEMENT:

1. **Betriebssystem-Updates aus Standard Repositories der Distribution**
2. **Einbindung eines Repositories von einem Drittanbieter auf Kundenwunsch**
3. **Updates von speziellen, auf Kundenwunsch installierten Anwendungen**

i Punkt 1 ist in der SERVICE CARD enthalten. Die Punkte 2 und 3 verursachen als Zusatzleistungen weitere Kosten. Es gelten die u. g. technischen Voraussetzungen*. Weitere Informationen sind dem Datenblatt Patchmanagement zu entnehmen – *siehe Anlage Datenblatt Patchmanagement.*

REDUZIERTE KOSTENSÄTZE FÜR SERVICE CARD INHABER:

- **100,- EUR** Stundensatz innerhalb der Geschäftszeiten 8 – 17 Uhr
- **149,- EUR** Stundensatz außerhalb der Geschäftszeiten

BACKUP DER KONFIGURATION:

1. **Für alle von uns betreuten Linux-/Unix-Systeme, Router, Switches und Firewalls**
2. **Sicherung der üblichen Systemkonfigurationsdateien im Basisumfang enthalten**
3. **Weitreichendere bzw. individuelle Lösungen nach Absprache gegen evtl. Mehrpreis möglich**

i Die genannten Punkte 1 und 2 sind durch die SERVICE CARD abgedeckt. Der Punkt 3 verursacht als Zusatzleistung weitere Kosten. Es gelten jedoch die u. g. technischen Voraussetzungen*. Weitere Informationen sind dem Datenblatt Sicherung von Konfigurationsdateien zu entnehmen – *siehe Anlage Datenblatt Sicherung von Konfigurationsdateien.*

ZENTRALES LOGMANAGEMENT:

1. **Für alle Linux-/Unix- und Windows-Systeme, Router, Switches sowie Firewalls**
2. **Sicherung der üblichen System- beziehungsweise Event-Logs im Basisumfang enthalten**
3. **Weitreichendere bzw. individuelle Lösungen nach Absprache gegen evtl. Mehrpreis möglich**

Die genannten Punkte 1 und 2 sind durch die SERVICE CARD abgedeckt. Der Punkt 3 verursacht als Zusatzleistung weitere Kosten. Es gelten jedoch die u. g. technischen Voraussetzungen*. Weitere Informationen sind dem Datenblatt zentrales Logmanagement zu entnehmen – *siehe Anlage Datenblatt zentrales Logmanagement.*

IM VERGLEICH:

KLASSISCHE CLOUDANGEBOTE

INFOSERVE RECHENZENTRUM & CLOUD

INFOSERVE RECHENZENTRUM & CLOUD
+ INFOSERVE SERVICE CARD

Verantwortungsbereich Kunde

Verantwortungsbereich INFOSERVE

*) TECHNISCHE VORAUSSETZUNGEN:

1. **Erreichbarkeit der betreffenden Systeme und Dienste**
2. **Zugriffsmöglichkeiten auf das Cloud Panel bzw. die Systeme für unsere Technik**

ALLGEMEINES

Unsere Technik muss die betreffenden Systeme und Dienste erreichen sowie auf die Systeme per VM-Konsole im Cloud Panel und über die jeweilige externe IPv4-IP-Adresse per Remote-Zugang (SSH bzw. RDP) zugreifen können.

Falls die Systeme von Ihnen im Cloud Portal selbst bereitgestellt werden sollten, sind von Ihnen die entsprechenden Zugänge für die INFOSERVE Technik einzurichten. Denken Sie dabei bitte immer daran, die Verbindungen durch die Cloud Firewall abzusichern.

Aus Sicherheitsgründen empfehlen wir ausdrücklich, Zugriffe von außen nur auf die erforderlichen externen IP-Adressen bzw. Ports in der Cloud Firewall freizuschalten. Dies gilt insbesondere für RDP-Zugänge. SSH-Zugänge sollten weiterhin ausschließlich eine SSH-Public-Key-Authentifizierung erlauben.

Die IP-Adresse, von der wir zugreifen werden, und unseren SSH-Public-Key erhalten Sie von uns im Rahmen der Bereitstellung Ihrer SERVICE CARD.

DOKUMENTATION

Die initial von INFOSERVE erstellte Dokumentation beschreibt die Systemumgebung zum Zeitpunkt des Projektabschlusses gemäß der entsprechenden Auftragsbestätigung. Soll die Dokumentation von INFOSERVE auf dem aktuellen Stand gehalten werden, was zugleich eine Voraussetzung für Supportleistungen seitens INFOSERVE darstellt, so ist INFOSERVE über vom Kunden durchgeführte Änderungen zu informieren.

MONITORING

1. **Check VM (hostcheck/ping)**
   Das System muss über externe IPv4-Adresse für INFOSERVE erreichbar sein.
2. **Check externer Service**
   Die Voraussetzung des Punkts 1 muss erfüllt sein und der jeweilige Port muss für INFOSERVE erreichbar sein.
3. **Checks Systemzustand – Standard-Umfang (Disk, Load)**
   Die Voraussetzungen der Punkte 1 und 2 müssen erfüllt sein. Weiterhin gilt:
   Für die Überwachung des Systemzustands ist aus Sicherheitsgründen die Bereitstellung einer Firewall-/VPN-Appliance erforderlich, durch die Ihnen zusätzliche Kosten entstehen können. Bei der Firewall-/VPN-Appliance handelt es sich um eine grundsätzlich zubuchbare Option, welche die Konfiguration von Netzwerk-VPNs ermöglicht und einen leistungsfähigen Paketfilter bietet. So werden auch Systeme innerhalb eines privaten Netzwerks überwachbar, wobei hierfür evtl. die Bereitstellung einer Monitoring-Satelliten-VM erforderlich wird, wodurch weitere Kosten entstehen.
4. **Weitere Checks auf Kundenwunsch**
   Im Gegensatz zu den Punkten 1 bis 3 sind diese nicht im Umfang der SERVICE CARD enthalten, d. h. durch die damit verbundenen Aufwände entstehen Ihnen zusätzliche Kosten.
   Die Voraussetzungen der Punkte 1 bis 3 müssen erfüllt sein. Der Check muss auch in Verbindung mit der eingesetzten Monitoring-Lösung realisierbar sein.

PATCHMANAGEMENT

In der SERVICE CARD ist das Patchmanagement in Form der Installation von Betriebssystem-Updates enthalten. Dieses umfasst alle Anwendungen, die aus dem Standard-Repository der jeweiligen Linux-Distribution installiert wurden, bzw. alle Anwendungen, die von den Windows Updates berücksichtigt werden.

Nicht enthalten ist hingegen das Patchmanagement von auf ausdrücklichen Kundenwunsch installierten Anwendungen, die nicht in die o. g. Kategorien fallen, wie z. B. im Falle einer Installation aus Dritthersteller-Repositories.

Aufgrund der heutigen Software-Komplexität und der möglichen Wechselwirkungen zwischen der Betriebssystem- und Anwendungsebene können wir leider nicht ausschließen, dass es infolge der Installation von Patches auf Betriebssystemebene zu Problemen mit Ihrer Anwendung kommen kann.

Das Risiko ist für die nicht von der SERVICE CARD abgedeckten Anwendungsfälle entsprechend höher.

Da wir hierauf keinen Einfluss haben, können wir evtl. entstehende Probleme auch nicht verantworten. Wir müssen Sie als Betreiber der jeweiligen Anwendung daher bitten, deren Funktionalität nach den Updates zu überprüfen bzw. diese im Fehlerfall wiederherzustellen. Bei der Fehlerbehebung können wir Sie natürlich kostenpflichtig unterstützen.

Anlagen:

- *Datenblatt Monitoring*
- *Datenblatt Patchmanagement*
- *Datenblatt Backup der Konfiguration*
- *Datenblatt zentrales Logmanagement*

Ihr Sorglos-Paket!

DATENBLATT MONITORING

INFOSERVE
>eurodata-Gruppe

Auf diesem Blatt können Sie festhalten, welche Ihrer Dienste wie überwacht werden sollen, und wie wir bei Auffälligkeiten reagieren sollen. Mögliche Reaktionen sind:

Reaktion	Was wir tun
Beheben	Wir versuchen, das Problem eigenständig zu lösen, z.B. durch Festplattenvergrößerung. Dadurch können Kosten entstehen.
SMS	Wir schicken den Ansprechpartnern eine SMS an die hinterlegte Handynummer.
Mail	Wir schreiben den Ansprechpartnern eine Mail.
Telefon	Wir versuchen, die Ansprechpartner auf der Büronummer anzurufen, sprechen ggf. auf Mailboxen, oder schicken bei Nichterreichen eine Mail.
Handy	Wir versuchen, die Ansprechpartner auf dem Handy anzurufen, sprechen ggf. auf Mailboxen, oder schicken bei Nichterreichen eine Mail.
Beheben + Mail	Wir versuchen, das Problem zu lösen, und informieren Sie währenddessen bzw. danach per Mail.
Beheben + Telefon	Wir versuchen, das Problem zu lösen, und informieren Sie währenddessen bzw. danach telefonisch unter Ihrer Büronummer.
Beheben + Handy	Wir versuchen, das Problem zu lösen, und informieren Sie währenddessen bzw. danach telefonisch auf Ihrem Handy.
-	Wir bestätigen die Warnung, ergreifen sonst aber keine Initiative.

ANSPRECHPARTNER

Bitte nennen Sie uns die Ansprechpartner, die wir in dieser Reihenfolge vom ersten bis zum letzten zu erreichen versuchen. Mails werden immer an alle geschickt. In der Notiz können Sie frei Wünsche äußern, z.B. "Nachts nur Mail". Die Notiz hat Vorrang vor den übrigen Vereinbarungen.

Erster Ansprechpartner	Zweiter Ansprechpartner	Dritter Ansprechpartner	Vierter Ansprechpartner
Name	Name	Name	Name
Mail	Mail	Mail	Mail
Telefon	Telefon	Telefon	Telefon
Handy	Handy	Handy	Handy
Notiz	Notiz	Notiz	Notiz

Sie können unten pro System und Dienst, der darauf läuft, Schwellwerte festlegen, ab wann gewarnt werden soll (noch unkritisch) und ab wann wir alarmiert werden sollen (kritisch!). Außerdem legen Sie fest, wie wir "werktags" (an Werktagen zwischen 7 und 18 Uhr) oder "sonst" (in der übrigen Zeit, also nachts, an Wochenenden und Feiertagen, nur SLA Premium) reagieren sollen. Als Beispiel haben wir unsere Standardschwellwerte und -reaktionen für Linux und Windows angegeben. Sie können die Standards abändern und darunter Ihre eigenen Schwellwerte und Reaktionen definieren.

STANDARDPARAMETER

Unsere Standardüberwachung für Linux- und Windows-VMs. Wenn Sie nichts anderes vereinbaren möchten, schreiben Sie unten nur den Namen des Systems auf und in die Spalte "Dienst" den Text "wie Standard".

System	Dienst	Warnen ab	Reaktion werktags	Reaktion sonst	Kritisch ab	Reaktion werktags	Reaktion sonst
Beispiel für eine Linux-VM	hostcheck (ping)	80% Paketverluste	SMS	SMS	100% Paketverluste	SMS	SMS
	disk (Standard)	90% Füllstand	SMS	SMS	95% Füllstand	SMS	SMS
	load	10 / 10 / 5 (1-5-15)	-	-	20 / 20 / 15 (1-5-15)	-	-
	swap	80% Füllstand	-	-	90% Füllstand	-	-
	uptime	(nur zur Information)	-	-	-	-	-
	ntp-time	300s	-	-	600s	-	-
	updates (Patch Mgm	neue reguläre Upd.	Beheben	-	neue kritische Upd.	Beheben	-
Beispiel für eine Windows-VM	hostcheck (ping)	80% Paketverluste	SMS	SMS	100% Paketverluste	SMS	SMS
	disk (Standard)	90% Füllstand	SMS	SMS	95% Füllstand	SMS	SMS
	load	90%	-	-	95%	-	-

ÜBERWACHUNG IHRER SYSTEME

System	Dienst	Warnen ab	Reaktion werktags	Reaktion sonst	Kritisch ab	Reaktion werktags	Reaktion sonst

DATENBLATT PATCHMANAGEMENT

PATCHMANAGEMENT LINUX SERVER

Wir bieten Patchmanagement für Linux Server Systeme aktuell für die Distributionen Rocky Linux, Debian und Ubuntu LTS an. Andere Linux-Distributionen werden hingegen nicht von uns unterstützt.

Patches für Rocky Linux werden manuell in einem zweiwöchentlichen Zyklus, Patches für Debian und Ubuntu Systeme hingegen automatisch installiert.

Alternativ kann die Installation der Patches im Rahmen eines individuell zu vereinbarenden Wartungstermines erfolgen. So können Auswirkungen auf den Produktionsbetrieb, wie beispielsweise ein eventuell erforderlicher Neustart und die damit verbundene Downtime, auf einen akzeptablen Zeitraum verschoben werden. Bitte beachten Sie, dass ein Wartungstermin außerhalb unserer regulären Geschäftszeiten die Berechnung des entsprechend höheren Stundensatzes zur Folge hat.

PATCHMANAGEMENT MICROSOFT WINDOWS SERVER

Das Patchmanagement für die von uns angebotenen Windows Server Versionen umfasst alles, was Microsoft per Windows Server Update Services (WSUS) für diese anbietet. Hierüber erhalten wir auch die Information, dass neue Patches vorliegen.

Wir stellen im Rahmen des Patchmanagement sicherheitsrelevante Patches sowie Rollups bereit. Jedoch sind keine Service Packs enthalten, da es sich bei diesen um Installationen handelt, die gesondert heruntergeladen und installiert werden müssen.

Der Patch-Mechanismus sieht die Erstellung einer lokalen Sicherheitsrichtlinie vor, durch welche eine unbeaufsichtigte Installation in den Nachtstunden im Fenster zwischen 0 und 3 Uhr konfiguriert wird. Der Neustart erfolgt automatisiert nach Einspielen der Patches.

PATCHMANAGEMENT APPLIANCE

Sollte INFOSERVE die Administration der Appliance übernehmen, so fällt hierunter auch das Patchmanagement, sofern dies technisch möglich ist.

Übernehmen Sie hingegen die Administration der Appliance, so fällt auch das Patchmanagement in Ihren Verantwortungsbereich.

ALLGEMEINE HINWEISE

Im Patchmanagement ist die Installation von Betriebssystem-Patches enthalten. Dieses umfasst alle Anwendungen, die aus dem Standard-Repository der jeweiligen Linux-Distribution installiert wurden, bzw. alle Anwendungen, die von den Windows Updates berücksichtigt werden.

Nicht enthalten ist hingegen das Patchmanagement von auf ausdrücklichen Kundenwunsch installierten Anwendungen, die nicht in die oben genannten Kategorien fallen, wie beispielsweise im Falle einer Installation aus Dritthersteller-Repositories.

Aufgrund der heutigen Software-Komplexität und der möglichen Wechselwirkungen zwischen der Betriebssystem- und Anwendungsebene können wir leider nicht ausschließen, dass es infolge der Installation von Patches auf Betriebssystemebene zu Problemen mit Ihrer Anwendung kommen kann.

Da wir hierauf keinen Einfluss haben, können wir eventuell entstehende Probleme auch nicht verantworten. Wir müssen Sie als Betreiber der jeweiligen Anwendung daher bitten, deren Funktionalität nach den Updates zu überprüfen beziehungsweise diese im Fehlerfall wiederherzustellen. Bei der Fehlerbehebung können wir Sie natürlich kostenpflichtig unterstützen.

DATENBLATT SICHERUNG VON KONFIGURATIONS-DATEIEN

Durch die Löschung oder fehlerhafte Änderungen von Konfigurationsdateien können ganze IT-Systeme beziehungsweise einzelne, darauf laufende Anwendungen leider schnell unbenutzbar werden oder bestimmte, teils geschäftskritische, Leistungen nicht mehr erbringen.

Sofern vorhanden, kann man aus den Backups des Systems – beispielsweise einer virtuellen Maschine – das komplette System und abhängig von der verwendeten Backup-Lösung oft auch die betroffene Konfigurationsdatei wiederherstellen.

Dabei handelt es sich aber um einen verhältnismäßig aufwendigen Prozess, denn schließlich handelt es sich oft nur um eine einzelne Änderung in einer Konfigurationsdatei. Nicht selten ist auch nicht mehr das genaue Datum der Änderung bekannt, sodass sogar mehrere Backups wiederhergestellt und durchsucht werden müssen, bis die korrekt funktionierende Version der betroffenen Konfigurationsdatei gefunden wird.

All dieser Aufwand für die Korrektur einer kleinen, aber verhängnisvollen Änderung kann deshalb einen erheblichen Zeitraum in Anspruch nehmen, einen Zeitraum, in welchem möglicherweise ein für Sie entscheidender Geschäftsprozess nicht zur Verfügung steht und Ihnen dadurch erhebliche Kosten beziehungsweise Umsatzverluste entstehen!

Durch die in der INFOSERVE SERVICE CARD PLATIN enthaltene Sicherung Ihrer Konfigurationsdateien können diese schnell und unkompliziert bei Bedarf wiederhergestellt werden.

Unterstützt werden von uns betreute Linux-/Unix-Systeme, Router, Switches und Firewalls. Im Basisumfang ist die Sicherung der üblichen Systemkonfigurationsdateien, wie man sie beispielsweise bei Linux/Unix im Verzeichnis /etc vorfindet, enthalten. Weitreichendere Sicherungen und bei Bedarf auch für Ihre konkreten Anwendungsfälle maßgeschneiderte Sicherungslösungen richten wir gerne in Absprache mit Ihnen zu einem von der jeweiligen Lösung abhängigen Mehrpreis ein.

DATENBLATT ZENTRALES LOGMANAGEMENT

Leider muss man vermehrt aus den Medien von Unternehmen erfahren, deren IT-Infrastruktur kompromittiert wurde. Infolgedessen werden Daten entwendet beziehungsweise verschlüsselt, die betroffenen Unternehmen erpresst, ihre IT-Infrastruktur gezielt an bestimmten Stellen oder gar komplett zerstört. Ob die Motivation der Angreifer nun aus blinder Zerstörungswut, ideologischer Natur oder finanziellen Interessen heraus motiviert ist, für die betroffenen Unternehmen bedeuten die Folgen leider nicht selten Reputationsverlust, Ermittlungen - je nach eigenem Verschulden in Form versäumter Maßnahmen hinsichtlich IT-Sicherheit - durch die Strafverfolgungsbehörden auch gegen das betroffene Unternehmen selbst und Folgekosten, die mitunter die Existenz des Unternehmens bedrohen können.

Die Angreifer sind dabei leider oft nicht zu identifizieren, schließlich haben sie größtes Interesse daran, ihre Identität zu verschleiern. Deshalb führen sie im Rahmen des Angriffs entsprechende Maßnahmen durch. Eine zentrale und in aller Regel erste Maßnahme ist es deshalb, mögliche Spuren in den Log-Dateien durch deren Löschung oder Änderung zu verwischen. So ist es kaum mehr möglich, im Rahmen der IT-Forensik Identität der Angreifer zu ermitteln und den Ablauf des Angriffs zu rekonstruieren. Gerade die Strafverfolgungsbehörden sind aber auf diese Informationen angewiesen. Die Gewährleistung unkompromittierter Logs wird deshalb von den einschlägigen IT-Versicherungen und durch für das Unternehmen geltende Compliance-Regeln zwingend gefordert.

Wie lässt sich dies aber sicherstellen? Wie können Sie Ihre Logs vor Angreifern schützen und somit Strafzahlungen gegen Ihr Unternehmen oder ausbleibende Versicherungsleistungen infolge der unterlassenen Absicherung Ihrer Logs gegen eine Kompromittierung durch Angreifer verhindern?

Durch die in der INFOSERVE SERVICE CARD PLATIN enthaltene Sicherung Ihrer Log-Dateien befinden sich diese zusätzlich außerhalb Ihrer IT-Infrastruktur zentral in einem der hochgesicherten INFOSERVE Rechenzentren.
Somit ist deren Validität auch nach einem Angriff auf ihre IT-Infrastruktur sichergestellt, und die Logs können somit unter anderem für die forensische Analyse und Beweisführung herangezogen werden.

Zusätzlich können ihre Log-Daten bei uns an zentraler Stelle aggregiert und analysiert werden, um aus der umfassenden, korrelierten Betrachtung von Informationen aus mehreren Quellen gegebenenfalls die entscheidenden Hinweise zu erhalten, die bei der isolierten Betrachtung der einzelnen Logs verborgen blieben.

Natürlich sind diese Möglichkeiten aber nicht nur im Falle eines Cyberangriffs, sondern auch bei der klassischen Fehlersuche äußerst hilfreich.

Unterstützt werden Linux-/Unix- und Windows-Systeme, Router, Switches sowie Firewalls, welche die technischen Voraussetzungen erfüllen. Im Basisumfang ist die Sicherung der üblichen System- beziehungsweise Event-Logs enthalten. Weitreichendere sowie bei Bedarf für Ihre konkreten Anwendungsfälle maßgeschneiderte Lösungen richten wir gerne in Absprache mit Ihnen zu einem von der jeweiligen Lösung abhängigen Mehrpreis ein.