JET SOFTWARE

JET-SECURITY

Identity- und Accessmanagement
für BS2000/OSD

Übersicht

Funktionen

Sicherheit

Produktbeschreibung

Pool-Verwaltung der Datenstationen unter einem Namen
Zusammenfassung der Kennungen zu Gruppen
Dynamische Veränderungen der Zugangsberechtigungen
Optionales Verhalten bei LOGON-Fehlversuchen
Vereinfachung der Verwaltung durch Zusammenfassung
Optionale Protokollierung der (auch ungültigen) LOGON-Versuche
Zentrale und revisionssichere Protokollierung aller Eingaben

JET SOFTWARE

Allgemeines

Das Gesamtpaket *JET-SECURITY* besteht aus mehreren Features:

- *LOGON-Security*
- *LOGON-Check*
- *JOINLIST*
- *FILE-Security*
- diverse *Security-EXITS*
- *CONSOLE*
- *WATCHDOG*
- *MESSAGE-Collect*

LOGON-*Security*

Für Benutzererkennungen können bei Einsatz des LOGON-*Security*-Verfahrens gezielt Einschränkungen des Systemzugangs vereinbart werden, welche über den Systemstandard hinausgehen. Dies muss bei dem Administrator (in der Regel von dem Systembetreuer der betreffenden Installation) für die entsprechenden Benutzerkennungen beantragt werden. Die vereinbarten Zugangsbeschränkungen werden zentral in der *Security*-Datei verwaltet.

- Übersicht
- Funktionen
- Sicherheit

Elementare Funktionen

- Pool-Verwaltung der Datenstationen unter einem Namen
- Ausschließung von definierten Datenstationen vom Teilnehmerbetrieb
- Verwendung eines JOB-Namens bei Dialog-LOGON erzwingen
- Dynamische Veränderung der Zugangsberechtigungen im laufenden Betrieb
- Einstellung der maximalen Lebensdauer eines LOGON-Kenwortes
- Abfrage eines zusätzlichen individuellen Kennwortes (CHECK-Kennwort) für einzelne Benutzer einer Benutzererkennung im Dialogbetrieb
- Verwaltung der Benutzereinträge und des Public-Space mit *JOINLIST*
- Zwangsprotokoll des Inhaltes der 'Datei mit den Zugangsberechtigungen' nach jeder Änderung mit Veränderungsstand
- Zusammenfassung der Kennungen zu Gruppen (generische Namen)
- Änderungszwang des CHECK-Kennwortes nach einer frei definierbaren Zeit
- Einstellbare maximale Anzahl von LOGON Fehlversuchen und optionales Verhalten
- Einstellung der maximal gleichzeitigen aktiven Dialog-TASKS
- Vereinfachung der Verwaltung durch Zusammenfassung von lokalen Prozessoren (HOST-Vorrechner) zu OWN-PROCESSOR
- Protokollierung der LOGON-Versuche (auch ungültige) in SYS-CONSLOG
- Zentrale und Dezentrale Administration möglich
- Mögliche Protokollierung aller Aktionen unter TSOS-Anwender und eingegebene Kommandos
- Zentrale und revisionssichere Protokollierung aller Kommando- und Systemeingaben von definierten Dialog-TASKS

Benutzererkennungen

Besteht für eine Benutzerkennung ein Eintrag in der SECURITY-Datei, wird ein LOGON nur noch in den angegebenen Betriebsarten (bzw. von den angegebenen Datenstationen) möglich. Grundsätzlich gibt es eine LOGON-Überprüfung auch für solche Benutzererkennungen, die keinen eigenen Eintrag in der SECURITY-Datei haben. Für Solche gelten die Paramterwerte, die bei der Anweisung SET-GLOBAL angegeben werden. Mit dieser Anweisung kann die Überprüfung der Verwendungsdauer durchgeführt werden, wobei auch die maximale Lebensdauer eines LOGON-Kennwortes festgelegt werden kann. Der Benutzer wird bei jedem LOGON über die restliche Verwendungsdauer verständigt.

JET SOFTWARE

Benutzer- und Stationsgruppen, POOL

Zur Vereinfachung der SECURITY-Verwaltung (Anweisungseingabe) und zur gezielten Zugangskontrolle gleichartiger Benutzergruppen, können Benutzererkennungen sowie Stationsnamen zu Gruppen zusammengefasst werden, wobei Stationen und Stationsgruppen mit gleichen Berechtigungen in einen „POOL" zusammengefasst werden können. Der POOL wird unter einem frei wählbaren Namen verwaltet (Anweisung: "SET POOL") und angesprochen (Anweisungen: "ADD-LOGON-SECURITY", "MODIFY-LOGON-SECURITY" und "SHOW-LOGON-SECURITY").

EXCEPT-Station

Mit der Anweisung "SET-GLOBAL" können Stationen bzw. Stationsgruppen vereinbart werden (Operand "EXCEPT -STATION"), von denen ein LOGON immer abgewiesen wird, außer wenn sie explizit in einem Benutzereintrag berechtigt sind und sich hier unter LOGON anmelden. Durch diese Funktion kann für bestimmte Stationen ganz oder teilweise der Teilnehmerbetrieb ($DIALOG) unterbunden werden (Stationen welche nur im Teilnehmerbetrieb-UTM-arbeiten sollen oder Wählleitungen).

Installation von LOGON-*Security*

Das BS2000/OSD muss mit den CLASS2-Options "TASKVECT=1" und "SYSVECT=1" in der Parameterdatei gestartet werden. Die Überprüfung der LOGON-Berechtigung wird in einem System-Exit (LOGON-Exit 030) vorgenommen, zusätzlich wird der P1-Exit verwendet. Die Administration (Verwaltung der Einträge zur LOGON-Berechtigung) erfolgt mit SDF-Anweisungen (SYSSTMT) für ein P1-Programm und mit SDF-Systemkommandos unter einer "normalen" Benutzerkennung.

Die SECURITY-Datei enthält die Einschränkungen des Systemzugangs für die einzelnen Benutzerkennungen. Diese Datei wird unter der Benutzerkennung SECURITY verwaltet und ist dort auch katalogisiert. Der Administrator des LOGON-Security-Verfahrens muss nicht notwendig auch der Systembetreuer sein, er braucht hier keine TSOS-Befugnisse. Unter TSOS sind keinerlei Dateien dieses Verfahrens gespeichert. Die Benutzerkennung SECURITY muss durch ein beliebiges LOGON-Kennwort geschützt sein und sollte sofort zusätzlich durch LOGON-Security gesichert werden.

Übersicht

Funktionen

Sicherheit

Verwaltung der SECURITY-Datei

Die SECURITY-Datei wird vom Administrator mit Hilfe von drei SDF-Systemkommandos und fünf SDF-Programmanweisungen verwaltet. Der Änderungsstand der SECURITY-Datei wird über eine Job-Variable automatisch fortgeschrieben.

Security-EXITS

In der Datei $SECURITY.SYSLNK.SECURITY.nnn sind neben den Exits für das SECURITY-Verfahren weitere Exits, überwiegend für Datei- und Systemüberwachung gespeichert (OPEN, ERASE, CATALOG, TSOS-Dialog-Kommandos).

JOINLIST

In Installationen mit mehreren Public-Volume-Sets und einer Vielzahl von Benutzerkennungen wird es immer schwieriger, die Zugriffsrechte und Abhängigkeiten darzustellen. Das Programm JOINLIST soll die Verwaltung der Benutzereinträge und des Public-Space verbessern.

Unsere Software ist seit über 30 Jahren aktiv im Einsatz bei:

- Deutschen Bundes- und Landesbehörden
- nationalen und internationalen Dienstleistern
- Sozial- und Privatversicherungen
- dem Mittelstand und Großunternehmen
- Landes-, Privat- und Großbanken

MADE IN GERMANY

LOGON-Check

Mit *LOGON-Check* kann die Zugangsüberprüfung für den Dialog-Zugang bedingt auf Personen (Inhaber des CHECK-Kennwortes) erweitert werden. Über Parameter kann zwingend die Hardcopy-Protokollierung für alle und für einzelne Einträge in den verschiedenen Anweisungen des Administratorprogrammes zugeschaltet werden, sodass Kommandoeingaben und Systemausgaben der definierten Dialog-Tasks zentral und revisionssicher protokolliert werden. *LOGON-Check* basiert nicht auf den System-Exits, sondern nutzt nur die TU-Schnittstelle, ist damit unabhängig von bestimmten BS2000/OSD-Versionen. Der Anwender wird nach einem erfolgreichen LOGON (BS2000/OSD-LOGON-Parameter und ggf. *LOGON-Security*) durch CHECK zur Eingabe seines individuellen Kennwortes aufgefordert. Die Informationen über den letzten, erfolgreichen und evt. fehlerhaften LOGON werden so ausgegeben. Nach Ablauf der maximalen Geltungsdauer des Kennwortes wird der Benutzer zur Eingabe eines neuen Kennwortes gezwungen. Wenn die maximale Anzahl von Fehlversuchen erreicht ist, kann ein Eintrag für den/die Benutzer gesperrt werden, nur der Security-Verwalter kann die Sperre dann aufheben.

FILE-Security

FILE-Security ersetzt die Exits für Dateiüberwachung (OPEN-, ERASE- und CATALOG-Exits) komplett durch ein neues Verfahren. Die Überwachung beinhaltet so auch ERASE- und CATALOG-Makros. Der Umfang der Überwachung und Protokollierung wird erweitert und durch eine Parameterdatei definiert.

- Übersicht
- Funktionen
- Sicherheit

CONSOLE

Mit dem Programm CONSOLE wird die Schnittstelle $CONSOLE des BS2000/OSD in $DIALOG (Teilnehmerbetrieb) für beliebige Benutzerkennungen unterstützt. Es kann im Dialog- und/oder Stapelbetrieb ablaufen, um Operatorkommandos einzugeben. Das Programm ist unabhängig von bestimmten BS2000/OSD-Versionen.

WATCHDOG

Mit dem Programm WATCHDOG kann der CPU-Verbrauch von Aufträgen (getrennt für Dialog- und Stapelaufträge) überwacht werden.

MESSAGE-Collect

Mit dem Verfahren *MESSAGE-Collect* sollen parallel zur Ausgabe von Meldungen in die vom BS2000/OSD genutzte Datei $TSOS.SYS.CONSLOG._, ausgewählte Meldungen in eine besondere COLLECT-Datei geschrieben werden. Die Meldungen aus *LOGON-Check* und den System-Exits von *LOGON-Security* werden automatisch gesammelt und so in die COLLECT-Datei ausgegeben. Der System- (bzw. SECURITY-)Verwalter kann bis zu 150 zusätzliche BS2000/OSD -Meldungsschlüssel angeben, die zusätzlich gesammelt werden sollen (z. B. für LOGON und LOGOFF).

Kontakt

Für weitere Informationen und für eine kostenlose Testversion wenden Sie sich bitte an:

JET-Software GmbH
Steinweg 1
D-64832 Babenhausen
Tel.: +49 (0) 6073-71140-3
E-Mail: info@jet-software.com
Web: www.jet-software.com