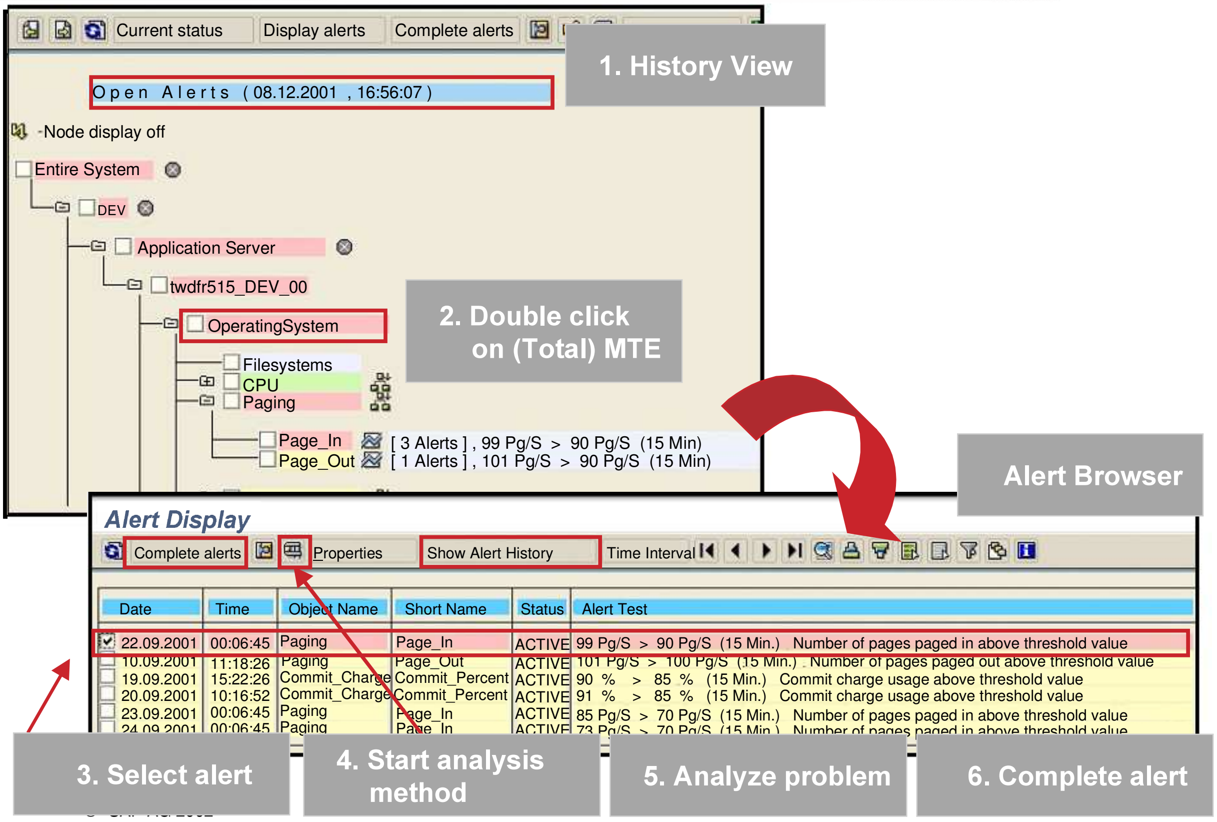
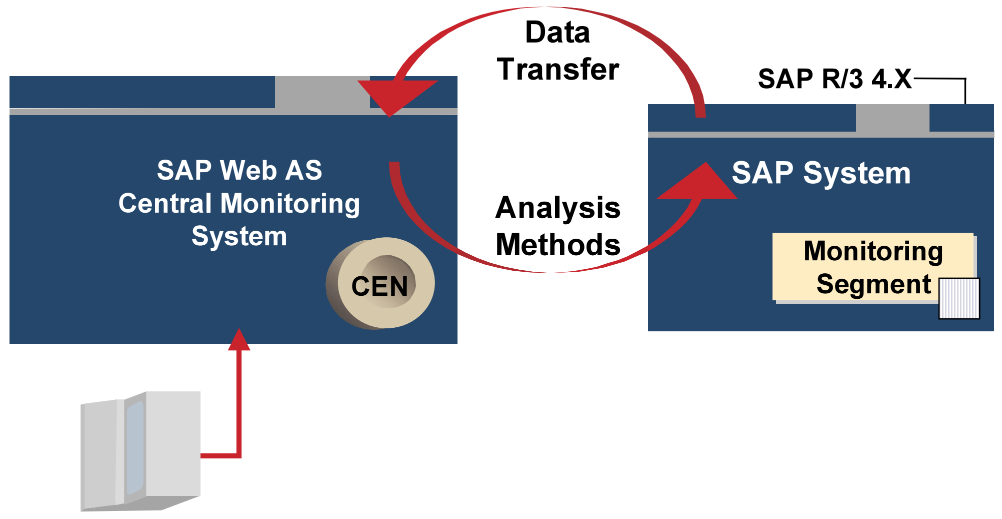
The Alert Browser



	Date	Time	Object Name	Short Name	Status	Alert Test
☑	22.09.2001	00:06:45	Paging	Page_In	ACTIVE	99 Pg/S > 90 Pg/S (15 Min.) Number of pages paged in above threshold value
□	10.09.2001	11:18:26	Paging	Page_Out	ACTIVE	101 Pg/S > 100 Pg/S (15 Min.) Number of pages paged out above threshold value
□	19.09.2001	15:22:26	Commit_Charge	Commit_Percent	ACTIVE	90 % > 85 % (15 Min.) Commit charge usage above threshold value
□	20.09.2001	10:16:52	Commit_Charge	Commit_Percent	ACTIVE	91 % > 85 % (15 Min.) Commit charge usage above threshold value
□	23.09.2001	00:06:45	Paging	Page_In	ACTIVE	85 Pg/S > 70 Pg/S (15 Min.) Number of pages paged in above threshold value
□	24.09.2001	00:06:45	Paging	Page_In	ACTIVE	73 Pg/S > 70 Pg/S (15 Min.) Number of pages paged in above threshold value

- You can easily process the alerts that occurred in the past in the *Open Alerts* view. By selecting an MTE in the tree, you open the Alert Browser, which displays a list of all alerts for the selected MTEs and all alerts below it in the tree. If you double-click the root of the tree, the system displays a list of all alerts in the tree, sorted by red and yellow alerts.
- Select an alert that you want to process. Then choose the pushbutton with the caliper. This starts the analysis method that is assigned to the MTE. The analysis method is a special tool that supports you when investigating problems. It can be transactions, or specially programmed function modules, or URL calls. You do not need to remember all of the special tools, but simply use the CCMS Alert Monitor as a central point of entry.
- After you have clarified the problem situation, choose F3 to return to the Alert Browser. Then choose *Complete Alerts*. The processed alert is removed from the list and is stored in a database table.
- Proceed in the same way with the remaining alerts, until the list is empty. When you next use your monitor, only the newly occurred alerts are displayed.
- If you want to display completed alerts again, choose *Show Alert History* in the Alert Browser. Completed alerts are displayed with the status *Done*.

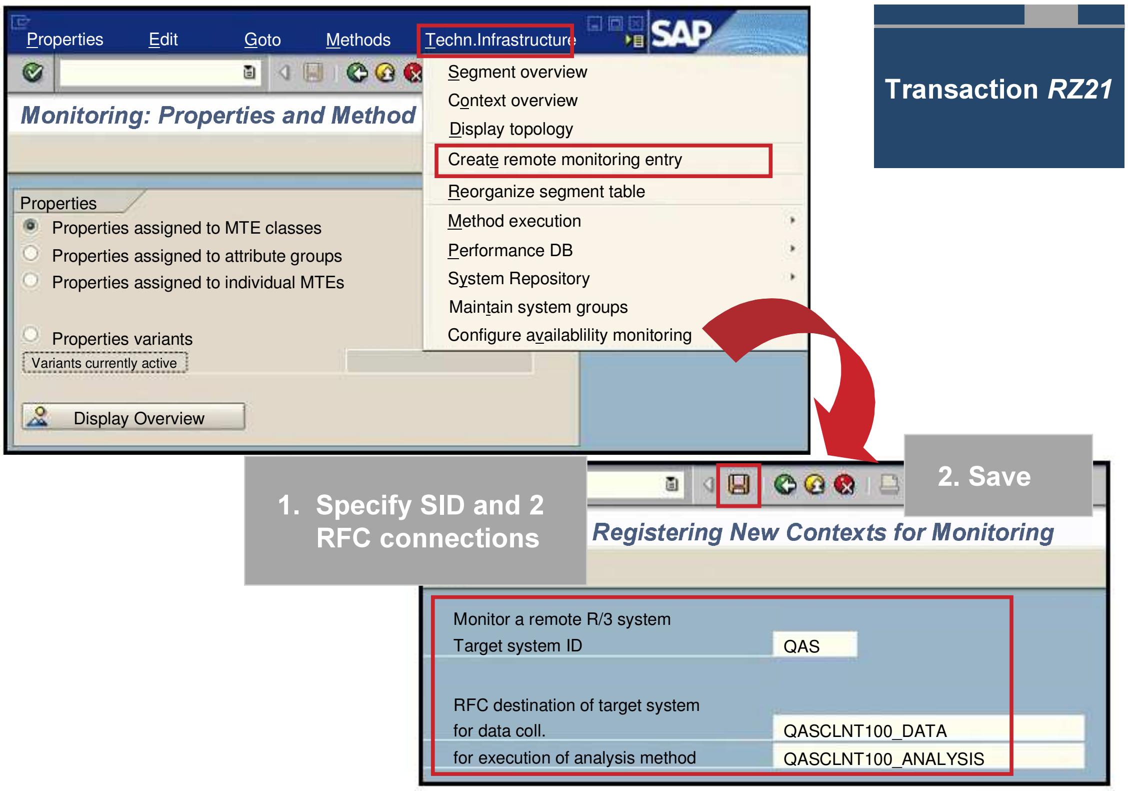
Include Remote Systems



- The monitors delivered by SAP display detailed monitoring data for the local SAP system. An advantage to central monitoring is that you can monitor the entire system landscape, and not just your local system.
- You can monitor all components that have a CCMS Alert Monitoring Infrastructure. SAP has delivered the infrastructure since SAP R/3 4.0. To be able to include components that do not have an infrastructure, you can use the CCMS agent programs SAPCM3X for SAP R/3 3.x and SAPCCMSR for non-SAP components.
- To include an SAP system in a central monitoring architecture, you must define an RFC connection over which the monitoring data for the SAP system can be transferred to the central monitoring system. The data collection is performed independently by the CCMS Alert Monitoring Infrastructure on the remote system.
- From a security point of view, it is recommended that you also define a second RFC connection between the system with which the analysis methods can be started in the remote system from the central monitoring system. If a problem occurs, you can therefore branch directly from the central monitor to the remote system to analyze the situation in more detail.

Include Remote Systems: Transaction *RZ21*

Transaction *RZ21*



Monitoring: Properties and Method

Properties
- ● Properties assigned to MTE classes
- ○ Properties assigned to attribute groups
- ○ Properties assigned to individual MTEs
- ○ Properties variants

Variants currently active

1. Specify SID and 2 RFC connections

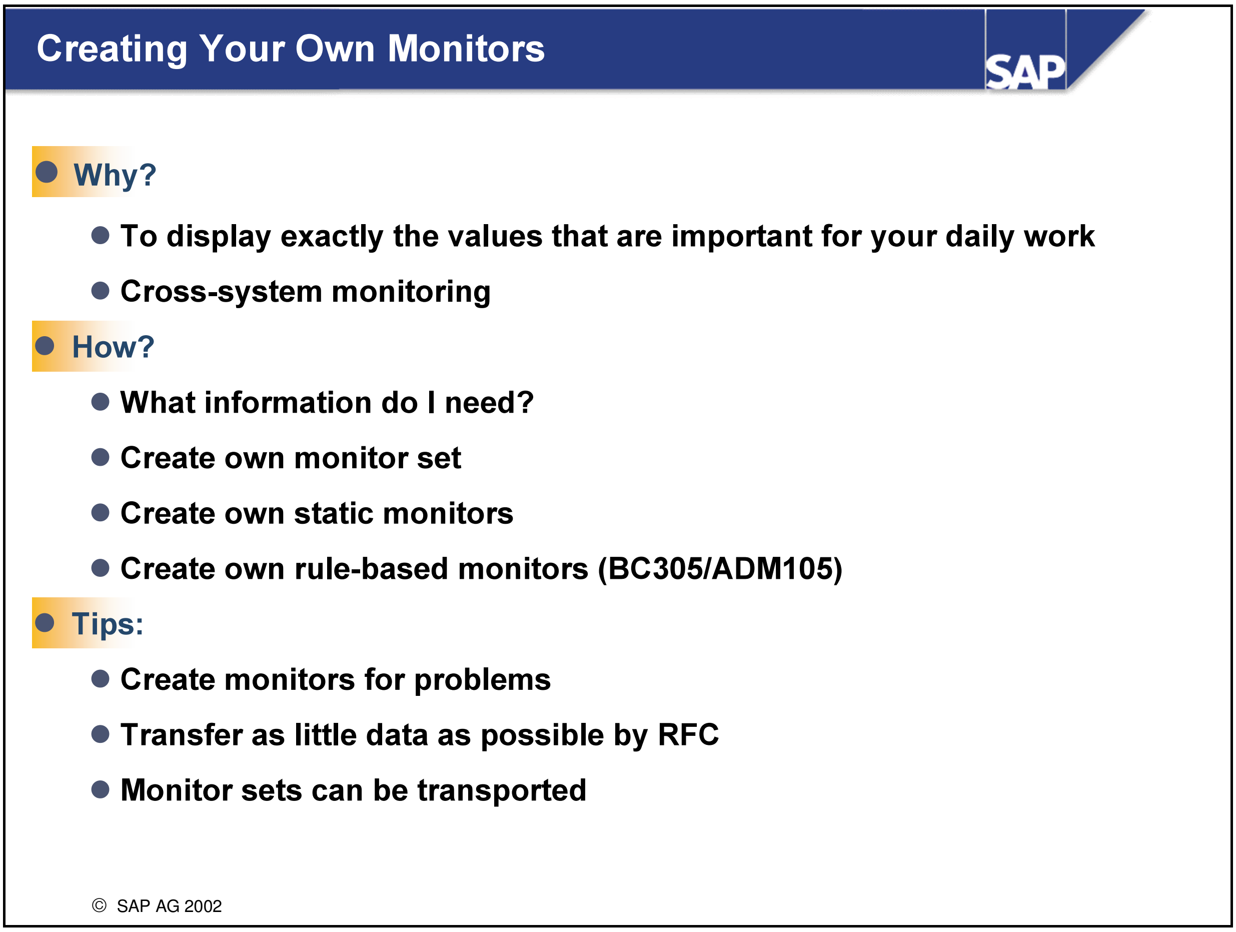
2. Save

Registering New Contexts for Monitoring

Monitor a remote R/3 system

Target system ID	QAS
RFC destination of target system	
for data coll.	QASCLNT100_DATA
for execution of analysis method	QASCLNT100_ANALYSIS

- SAP systems are included in the central monitoring system in transaction *RZ21*. You can start the transaction from the SAP Easy Access Menu by choosing *Tools* → *CCMS* → *Configuration* → *Alert Monitor*.
- In *RZ21*, choose *Technical Infrastructure* → *Create Remote Monitoring Entry*.
- Enter the SID of the SAP system to be monitored in the *Target System ID* field.
- Now create the two RFC connections from the central monitoring system to the monitored SAP system. Choose *Goto* → *RFC Connections*. The system displays transaction *SM59*. Create two RFC connections here. Note that the connection type is *3* (SAP R/3 - SAP R/3 communication).
- In the RFC connection for the transfer of the monitoring data, you can enter a CPI-C user with a password that is valid in the monitored SAP system. When the central monitoring system requests monitoring data from the monitored SAP system, it is provided without the need for authorization.
- In the RFC connection that is to be used for the start of the analysis method, do not enter a user, but rather check the field *Current User*. If an analysis method is started in the monitored system from the central monitoring system if problems occur, the caller must authorize himself or herself in the monitored system.
- Return to transaction *RZ21* by choosing *F3*. Enter the RFC connections that you created under *RFC destination of target system.* Choose *Save*. The SAP system can now be centrally monitored.



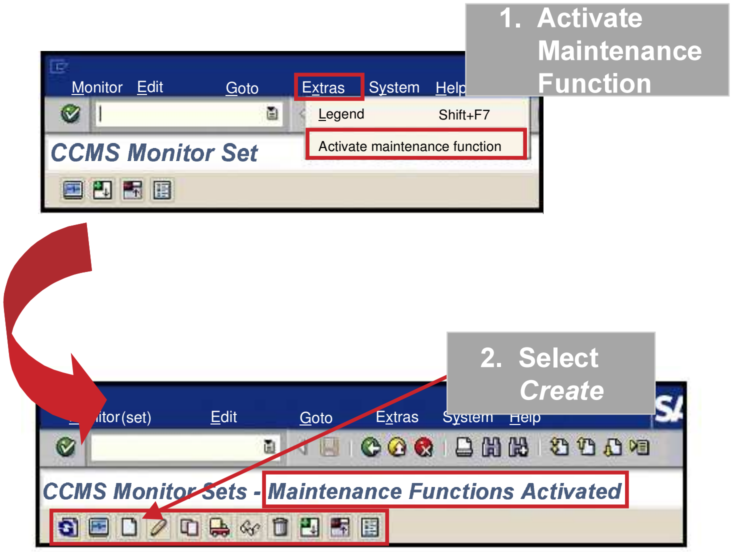
Creating Your Own Monitors

- Why?
  - To display exactly the values that are important for your daily work
  - Cross-system monitoring
- How?
  - What information do I need?
  - Create own monitor set
  - Create own static monitors
  - Create own rule-based monitors (BC305/ADM105)
- Tips:
  - Create monitors for problems
  - Transfer as little data as possible by RFC
  - Monitor sets can be transported

- For your regular work, you should create your own monitors that display precisely the cross-system or local data that you require for your work.
- The monitor sets and monitors delivered by SAP cannot be changed. You should therefore first create your own monitor set. You can then create your own, static monitors that display the required data. The second technique for creating your own monitors, rule-based monitors, is described in detail in the BC305/ADM105 course.
- Before you create your own monitor, you should clarify the purpose of the monitor. The monitor should display as little data as possible as concisely as possible. You must make a selection from the many hundreds of monitoring attributes that meets your requirements. A system overview monitor, for example, should contain the status of the last database backup or terminated updates as core indicators, but not details about the distribution of the dialog response time. You should create another monitor to display the response time.
- If data from the monitored SAP systems is also to be displayed, the quantities of data to be transferred can quickly become very large. A monitor that displays the complete monitoring data for two remote systems is unusable, as the data transfer lasts too long, especially if the remote systems have a heavy load. As a global guide value, use 10-20 monitoring attributes for each monitored instance in the central monitor.

Create Monitor Set

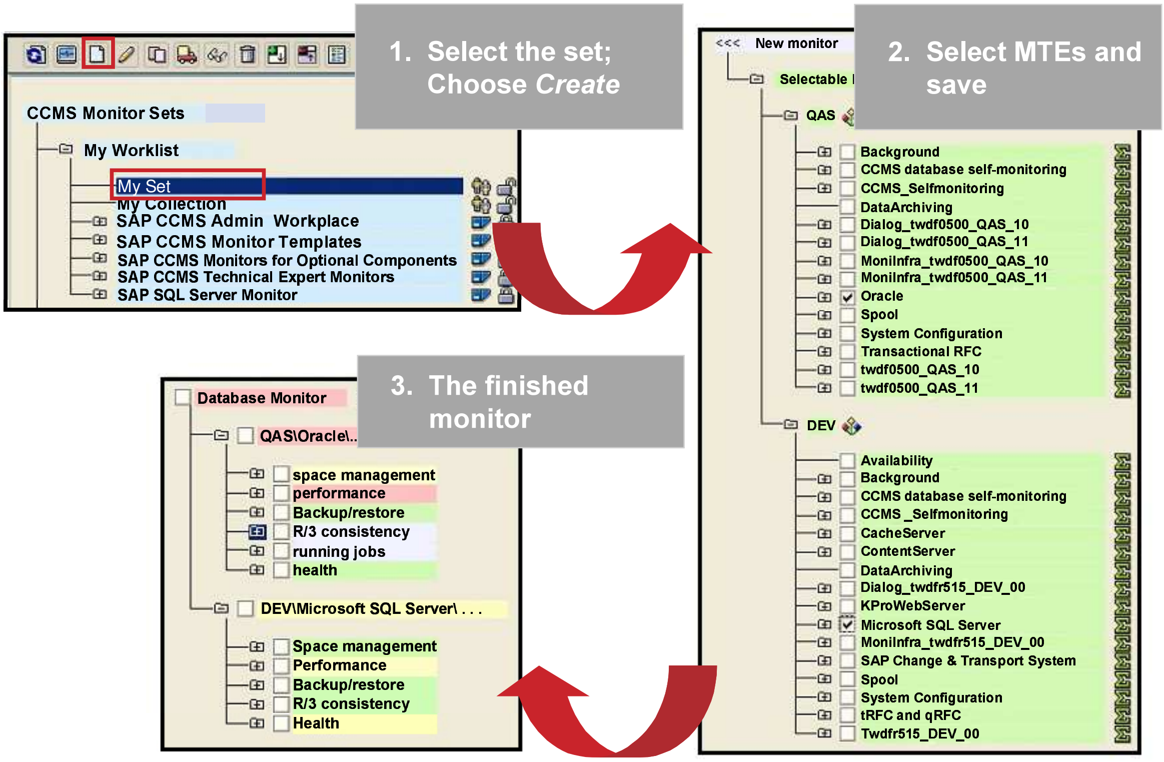
Transaction *RZ20*


1. Activate Maintenance Function
Monitor Edit Goto Extras System Help
Legend Shift+F7
Activate maintenance function
CCMS Monitor Set
2. Select *Create*
Monitor(set) Edit Goto Extras System Help
CCMS Monitor Sets - Maintenance Functions Activated

© SAP AG 2002

- The CCMS Alert Monitor (Transaction *RZ20*) is usually in display mode, in which you can open monitors, but cannot create or change monitors. To activate change mode, choose *Extras* → *Activate maintenance function* in transaction *RZ20*. *Maintenance Functions Activated* appears in the transaction heading. The system displays new pushbuttons for creating and changing monitors and monitor sets. Choose *Create* . The system asks whether you want to create a monitor set or a monitor. Select *Monitor set* and choose *Copy*. Enter a name for your monitor set. Note the naming convention that your monitor set should not begin with *SAP*.
- You can choose if other users can change your monitor set or not. You can also choose whether the set is displayed for other users in the CCMS Alert Monitor. After you have specified the set attributes, choose *Enter*. You have now created your own monitor set, into which you can either create new monitors or copy existing monitors.
- The monitor sets and monitors delivered by SAP cannot be changed. However, you can use them as stable templates. You can set whether or not an SAP monitor set should appear in the display mode of the CCMS Alert Monitor. If you want to hide an SAP monitor set, click on the set and then on the *Change* button. Remove the selection for *public*. The set can now no longer be seen in the display mode. You can change your selection in the change mode.

Static Monitors



1. Select the set; Choose *Create*

CCMS Monitor Sets

- My Worklist
  - My Set
  - My Collection
  - SAP CCMS Admin Workplace
  - SAP CCMS Monitor Templates
  - SAP CCMS Monitors for Optional Components
  - SAP CCMS Technical Expert Monitors
  - SAP SQL Server Monitor

2. Select MTEs and save

<<< New monitor

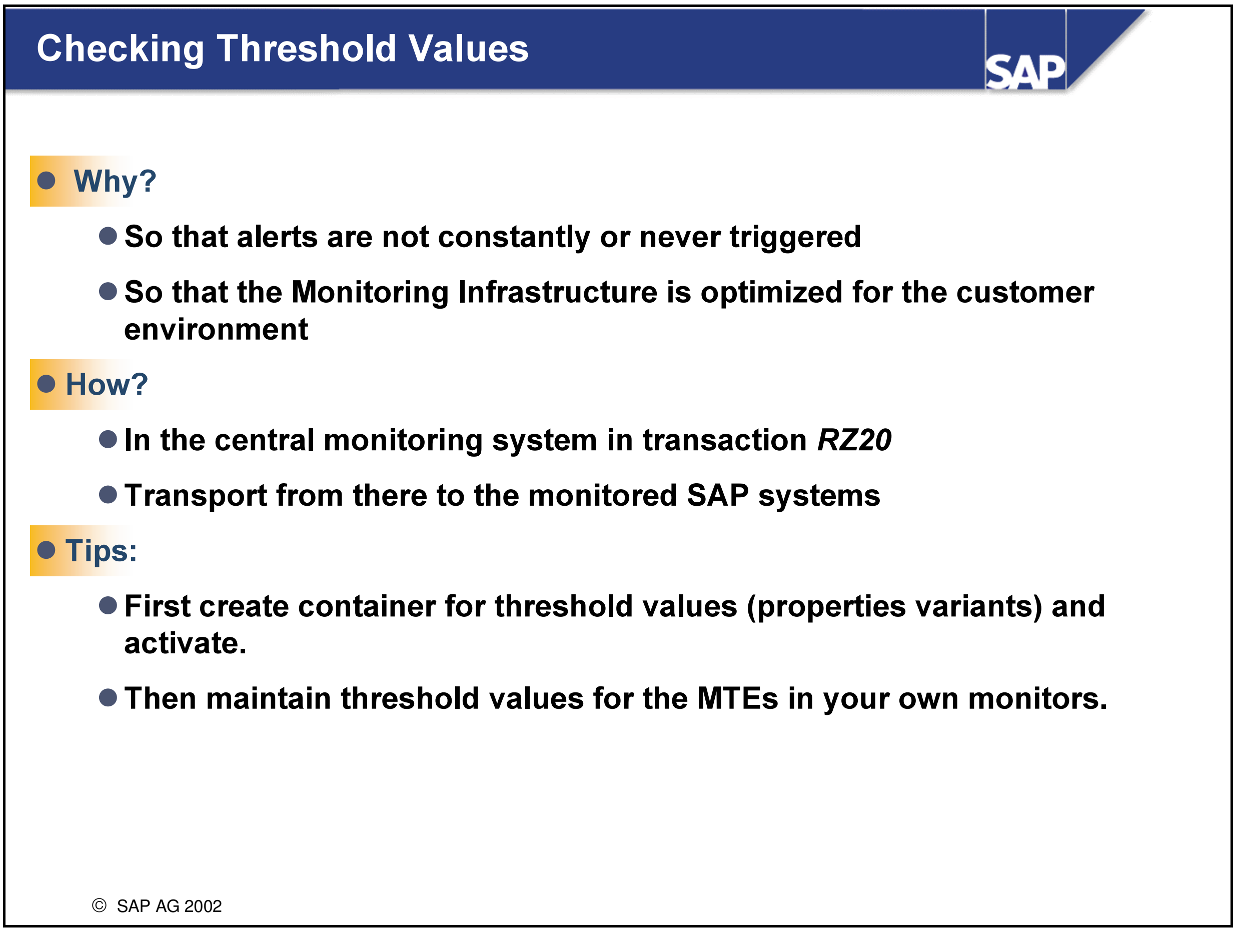
- Selectable
  - QAS
    - □ Background
    - □ CCMS database self-monitoring
    - □ CCMS_Selfmonitoring
    - □ DataArchiving
    - □ Dialog_twdf0500_QAS_10
    - □ Dialog_twdf0500_QAS_11
    - □ MonInfra_twdf0500_QAS_10
    - □ MonInfra_twdf0500_QAS_11
    - ☑ Oracle
    - □ Spool
    - □ System Configuration
    - □ Transactional RFC
    - □ twdf0500_QAS_10
    - □ twdf0500_QAS_11
  - DEV
    - □ Availability
    - □ Background
    - □ CCMS database self-monitoring
    - □ CCMS _Selfmonitoring
    - □ CacheServer
    - □ ContentServer
    - □ DataArchiving
    - □ Dialog_twdfr515_DEV_00
    - □ KProWebServer
    - ☑ Microsoft SQL Server
    - □ MonInfra_twdfr515_DEV_00
    - □ SAP Change & Transport System
    - □ Spool
    - □ System Configuration
    - □ tRFC and qRFC
    - □ Twdfr515_DEV_00

3. The finished monitor

□ Database Monitor

- □ QAS\Oracle\..
  - □ space management
  - □ performance
  - □ Backup/restore
  - □ R/3 consistency
  - □ running jobs
  - □ health
- □ DEV\Microsoft SQL Server\ . . .
  - □ Space management
  - □ Performance
  - □ Backup/restore
  - □ R/3 consistency
  - □ Health

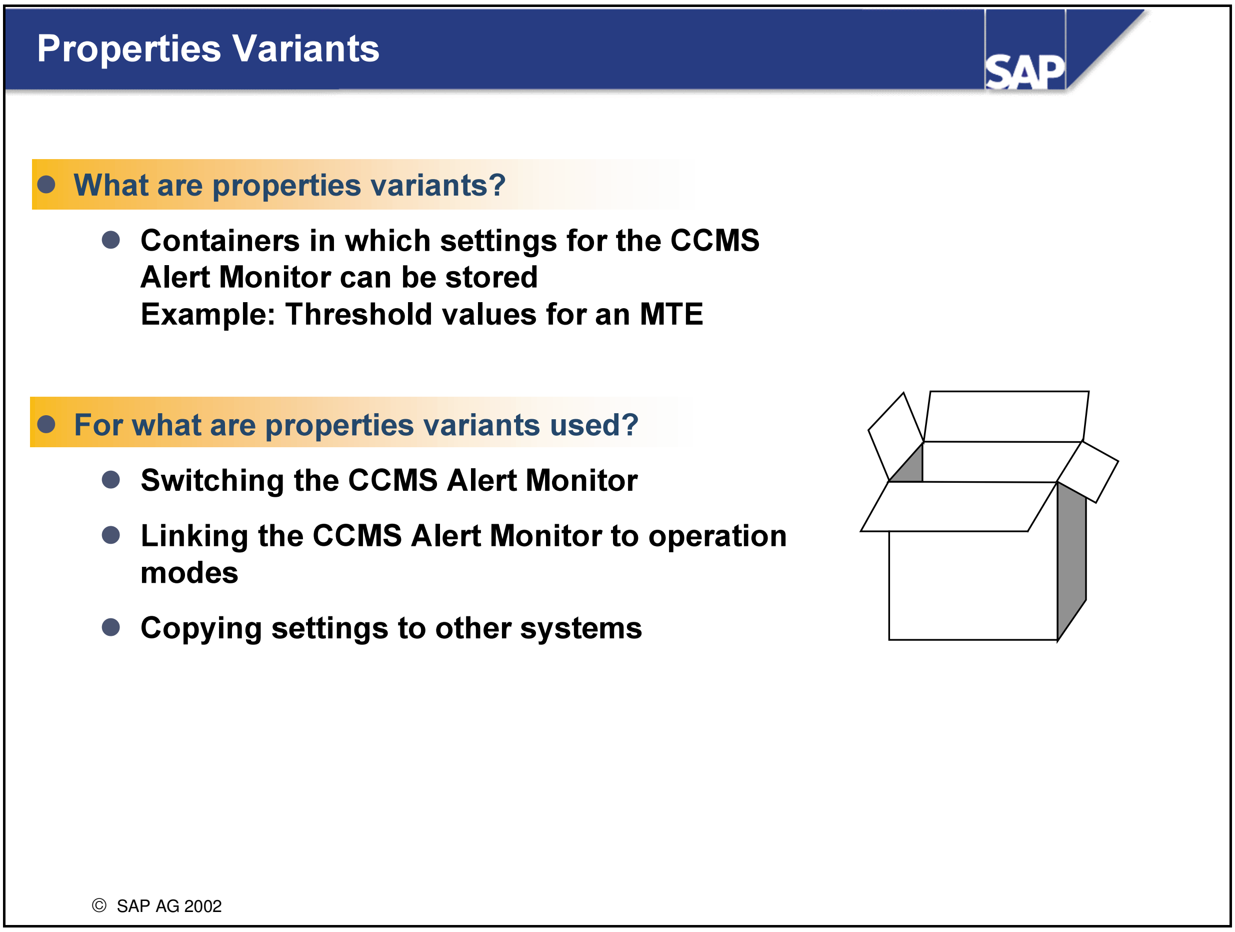
- Now create new monitors or copy existing monitors into your monitor set.
- To create new monitors in your set, select the set and choose *Create*. The system displays a selection screen in which all MTEs for all registered systems are displayed. Expand the tree structure and choose the MTEs that you want to display in your monitor by checking them. If an MTE is checked, all MTEs underneath it are automatically copied to the monitor. Take into account considerations about the number of MTEs.
- Choose *Save*. The system prompts you for a name for the new monitor, which you can then start by double-clicking it.
- The diagram shows a monitor that displays cross-system monitoring data from two SAP databases. You use this monitor in exactly the same way as the SAP standard monitors (current view, open alerts, Alert Browser).
- You can organize your monitor more clearly by using virtual nodes when selecting the MTEs. Virtual nodes allow you to structure your monitor. During the MTE selection, choose *Create* and then *Virtual Node*. You can choose any text for the virtual node. It should be as descriptive as possible. Complete your entry by choosing *Enter*. Your virtual node is inserted. You can now select any MTEs for inclusion in the monitor under this node. In the final monitor, these MTEs appear under the virtual node.



Checking Threshold Values

- **Why?**
  - **So that alerts are not constantly or never triggered**
  - **So that the Monitoring Infrastructure is optimized for the customer environment**
- **How?**
  - **In the central monitoring system in transaction *RZ20***
  - **Transport from there to the monitored SAP systems**
- **Tips:**
  - **First create container for threshold values (properties variants) and activate.**
  - **Then maintain threshold values for the MTEs in your own monitors.**

- Threshold values can be stored for a monitoring attribute. Threshold values determine when the monitoring attribute should trigger a yellow or a red alert, and when it should become green or yellow again. The CCMS Alert Monitoring Infrastructure is delivered preconfigured with threshold values recommended by SAP. You should check the threshold values, at least for the monitoring attributes that you consider to be important and that you have included in your own monitors. In this way, you customize the CCMS Alert Monitor optimally to your system environment. Otherwise, alerts can be constantly or never triggered, depending on whether the threshold value is too low or too high for your system environment.
- Threshold values must be stored locally in every system. However, instead of maintaining the same threshold values in every system, you should maintain the values in the central monitoring system and then distribute them to the monitored SAP systems using the transport system.
- The prerequisite for transporting the threshold values to other SAP systems is that you have stored them in properties variants.



Properties Variants

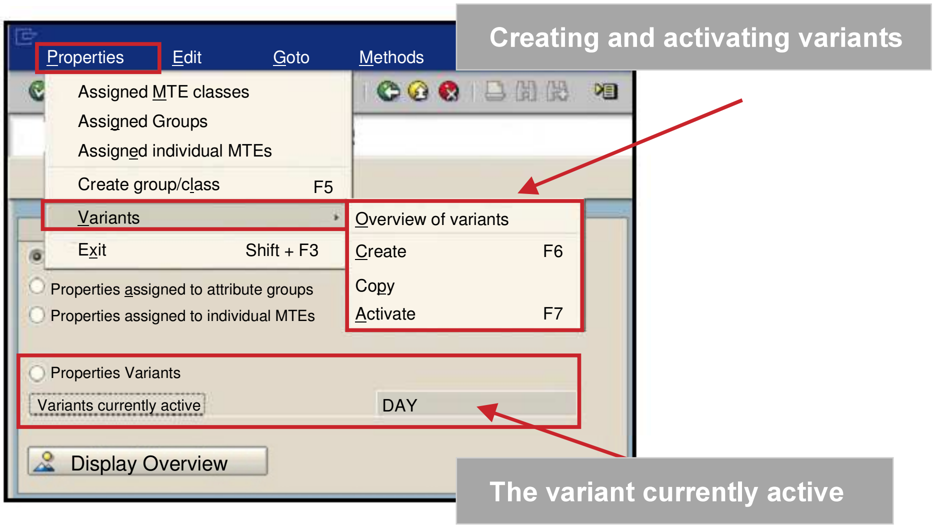
- **What are properties variants?**
  - **Containers in which settings for the CCMS Alert Monitor can be stored**
    Example: Threshold values for an MTE
- **For what are properties variants used?**
  - **Switching the CCMS Alert Monitor**
  - **Linking the CCMS Alert Monitor to operation modes**
  - **Copying settings to other systems**

© SAP AG 2002

- Properties variants are containers in which CCMS Alert Monitor settings, such as threshold values, can be stored.
- You can create as many properties variants as you like and store CCMS Alert Monitor settings in them. Exactly one properties variant with your settings is active at any time.
- Properties variants have three advantages:
  - You can manually switch from one properties variant to another for test purposes or to adjust the monitor to a special situation. This means that all monitor settings are automatically changed in accordance with the current properties variant.
  - You can connect a properties variant to an operation mode. In this way, the threshold value for the dialog response time is set to 1s during the day, while the threshold value is automatically increased to 10s after the switch to night operation, as there is usually no dialog processing during the night.
  - You can transport the contents of properties variants to other SAP systems using the transport system. For example, if you create a variant for production systems in the central monitoring system, and maintain the threshold values that are to apply for production systems there, you can then transport the variant to all production systems and activate the threshold values there.

Creating and Activating Properties Variants

Transaction *RZ21*



●
○ Properties assigned to attribute groups
○ Properties assigned to individual MTEs

○ Properties Variants
Variants currently active DAY

Creating and activating variants

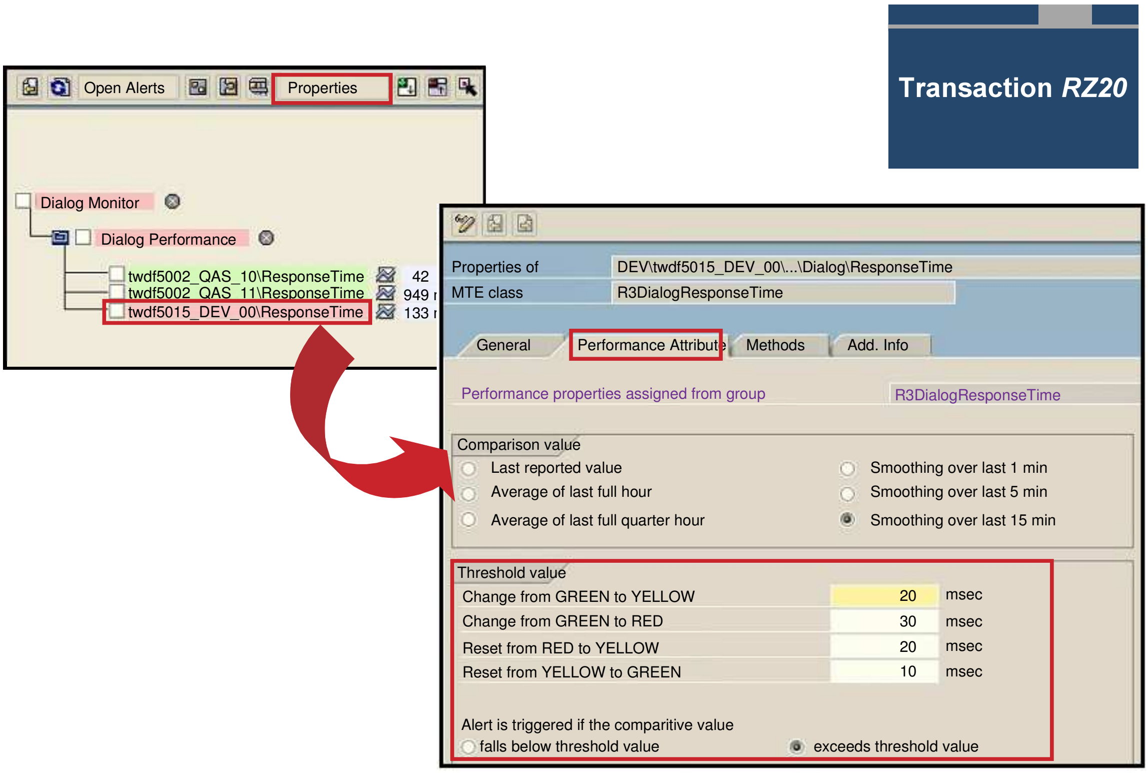
The variant currently active

© SAP AG 2002

- Properties variants are created in transaction *RZ21*. You can find the important functions for properties variants by choosing *Properties* → *Variants*.
- First, create your own properties variant. Choose *Properties* → *Variants* → *Create*. Enter a name and a description for the properties variant, and save it.
- Then choose *Properties* → *Variants* → *Activate*. Select your variant and choose *Enter*. Your properties variant is now active and is displayed on the initial screen of transaction *RZ21*. All threshold value settings that you make from now in the CCMS Alert Monitor are saved in the active variant.
- You can organize properties variants hierarchically. You can specify a parent variant when you create variants. If you do not specify another variant, the variant * is implicitly assumed to be the parent variant, whose parent variant, is, in turn, *SAP-DEFAULT*. The threshold values recommended by SAP are stored in *SAP-DEFAULT*. They cannot be changed.
- If no threshold value is maintained for a monitoring attribute in your variant, the system checks the parent variant. If this also has no threshold value, its parent variant is checked, and so on. Your properties variant is empty after it has been created. Therefore, after activation, the threshold values that are stored in the variant * or *SAP-DEFAULT* apply.
- The connection of properties variants to operation modes is performed in transaction *RZ04*. Select the operation mode and choose *Operation Mode* → *Change*. You can enter the desired properties variant in the field *Monitoring Properties Variant*. Save your entries.

Maintain Threshold Values

Transaction *RZ20*



- Dialog Monitor
  - Dialog Performance
    - twdf5002_QAS_10\ResponseTime 42
    - twdf5002_QAS_11\ResponseTime 949 r
    - twdf5015_DEV_00\ResponseTime 133 r

Properties of: DEV\twdf5015_DEV_00\...\Dialog\ResponseTime

MTE class: R3DialogResponseTime

General | Performance Attribute | Methods | Add. Info

Performance properties assigned from group R3DialogResponseTime

Comparison value

○ Last reported value ○ Smoothing over last 1 min

○ Average of last full hour ○ Smoothing over last 5 min

○ Average of last full quarter hour ● Smoothing over last 15 min

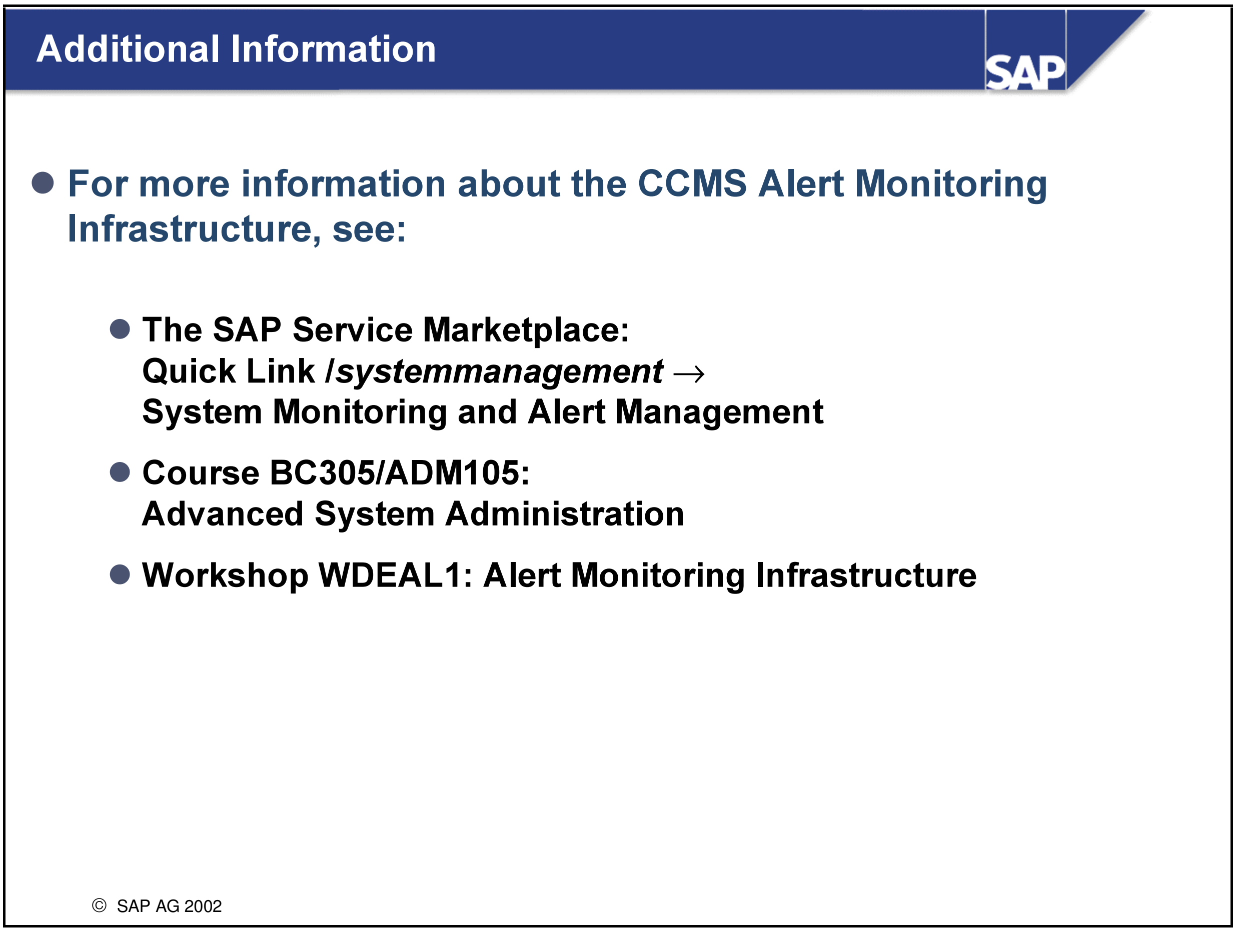
Threshold value

Change from GREEN to YELLOW	20	msec
Change from GREEN to RED	30	msec
Reset from RED to YELLOW	20	msec
Reset from YELLOW to GREEN	10	msec

Alert is triggered if the comparitive value

○ falls below threshold value ● exceeds threshold value

- After you have activated your properties variant, you can check the threshold values for the monitoring attributes that you regard as important and that you have included in your own monitors.
- To do this, open your monitor in the CCMS Alert Monitor (transaction *RZ20*). Select a monitoring attribute and choose *Properties*. The current tab page displays the valid threshold value definition.
- The thresholds for green to yellow and yellow to red are normally more sharply defined than the thresholds from red to yellow and yellow to green. In this way, you can avoid your monitor flickering, if the measured value is wavering around the threshold value. It is useful to give an “all clear” only once the situation has markedly improved.
- Choose *Display* <-> *Change*. You can now adjust the threshold values to your requirements. Save your settings.
- The threshold values are stored in the current properties variant. You can copy these settings to a transport request and transport them to other SAP systems. To transport the threshold values, choose *Properties* → *Variants* → *Overview of Variants* in transaction *RZ21*. In the overview of variants, choose *Variant* → *Transport.* By doing this, you create a transport request that can be transported to other SAP systems using the transport management system TMS.



Additional Information

- For more information about the CCMS Alert Monitoring Infrastructure, see:
  - The SAP Service Marketplace:
    Quick Link */systemmanagement* →
    System Monitoring and Alert Management
  - Course BC305/ADM105:
    Advanced System Administration
  - Workshop WDEAL1: Alert Monitoring Infrastructure

- For more information about the CCMS Alert Monitoring Infrastructure, see the SAP Service Marketplace. Use the Quick Link */systemmanagment* and choose *System Monitoring and Alert Management*.
- The course BC305/ADM105: Advanced System Administration introduces in particular configuring methods (analysis and auto reaction) and the use of rule-based monitors.
- The workshop WDEAL1 is a two-day workshop that covers the CCMS Alert Monitoring Infrastructure in detail. Among other topics, working with CCMS agents is explained. It is provided by SAP's international subsidiaries.

System Monitoring: Summary

You are now able to:

- Explain the concepts of the CCMS Alert Monitoring Infrastructure
- Configure and use the CCMS Alert Monitor for your regular system monitoring
- Check and adjust the threshold values for the monitoring attributes that are important for you

Exercises

No.	Exercises
1	**The CCMS Alert Monitor**
1.1	Start the CCMS Alert Monitor (transaction *RZ20*). Open the *Entire System* monitor from the *SAP CCMS Monitor Templates* monitor set. What is the current average dialog response time? What are the threshold values for this monitoring attribute? Switch to the *Open Alerts* view. Select all alerts that have occurred in the *Dialog* area. Process an alert from this list: • Start the analysis method for an alert. • Return to the Alert Browser and complete the alert. Does the alert still appear in the list? • How can you display the completed alert again?
2	**Include remote SAP systems in the central monitoring architecture**
2.1	As of now, your SAP system is the central monitoring system. Register the SAP system of your partner group in your system. To do this, get the details of a valid user with password from your partner group. Where can you see data from your partner group's SAP system?
3	**Create a properties variant**
3.1	Create your own properties variant, *TEST*, in your SAP system. Activate your properties variant.
4	**Create a monitor set**
4.1	Create your own monitor set, *System Monitoring*.
5	**Create a monitor**
5.1	Create your own cross-system monitor, *Core_information* that displays the most important system monitoring data. First consider which information is important for monitoring from your point of view. Remember that you should not display too many values for each SAP system.
5.2	Now create the monitor *Core_information*. The monitor should, as far as possible, display the desired data for your system and your partner group's system. Structure the monitor using virtual nodes.

6	**Maintain threshold values**
6.1	Open your *Core_information* monitor. Display all alerts for the entire monitor. Process an alert for the partner group’s system, as described in exercise 1.1. • Start the analysis method for an alert. • Return to the Alert Browser and complete the alert. Does the alert still appear in the list? • How can you display the completed alert again?
6.2	Maintain the threshold values for a monitoring attribute in your monitor. To do this, find a monitoring attribute from **your** SAP system, for which you can maintain the thresholds for: • Green to yellow • Green to red • Red to yellow • Yellow to green . Change these threshold values and save them. (Note: These threshold values can only be specified for performance monitoring attributes. There are two other monitoring attribute types, for which threshold values are specified in a different way.)
7	**Manual switch of properties variants**
7.1	Activate the *SAP-DEFAULT* properties variant in transaction *RZ21*. What is the threshold value for the MTE that you set in exercise 6.2?

No.	Solutions
1	**The CCMS Alert Monitor**
1.1	**Start the CCMS Alert Monitor (transaction *RZ20*).** Call the CCMS Alert Monitor (*Tools* → *CCMS* → *Control/Monitoring* → *Alert Monitor*, transaction *RZ20*). **Open the *Entire System* monitor from the *SAP CCMS Monitor Templates* monitor set.** Expand the *SAP CCMS Monitor Templates* set by choosing the + sign beside the set. Double click the *Entire System* set. **What is the current average dialog response time?** You can find the monitoring attribute for the average dialog response time by expanding, for example, the branch *<SID>* → *R/3 Services* → *Dialog* → *<Instance>*. Note that the monitor is in the *Current Status* view. **What are the threshold values for this monitoring attribute?** Select the monitoring attribute *ResponseTime* and choose *Properties*. The current threshold values are displayed on the *Performance Attribute* tab page. **Switch to the *Open Alerts* view.** Return to the monitor by choosing F3. Choose *Open Alerts*. **Select all alerts that have occurred in the *Dialog* area.** Double click the *Dialog* MTE. All alerts in this area are displayed in the Alert Browser. **Process an alert from this list:** • **Start the analysis method for an alert.** • **Return to the Alert Browser and complete the alert. Does the alert still appear in the list?** • **How can you display the completed alert again?** Select an alert in the list. Then choose *Start Analysis Method*. The system jumps from the monitor to a function that provides you with detailed data about the alert. Return to the monitor. Choose *Complete Alert*". The alert is removed from the list. To display an alert again, choose *Show Alert History*. Your completed alert has the status *DONE*. Note: It is possible that the system displays other alerts with the status *AUTO_COMPLETE*. These alerts were completed automatically by the system to keep the alert area free for new alerts.

2	**Include remote SAP systems in the central monitoring architecture**
2.1	**As of now, your SAP system is the central monitoring system.** **Register the SAP system of your partner group in your system. To do this, get the details of a valid user with password from your partner group.** **Where can you see data from your partner group's SAP system?** Get the details of a valid user with password from your partner group. Call the configuration transaction for the CCMS Alert Monitor (*Tools* → *CCMS* → *Configuration* → *Alert Monitor*, transaction *RZ21*). Choose *Technical Infrastructure* → *Create remote monitoring entry*. Under *Target System ID*, enter the <*SID*> of your partner group's system. Choose *Goto* → *RFC Connections*. Choose *Create*. Enter the following values: • RFC Destination: **<SID>_DATA** (Replace <SID> with the <SID> of your partner group's system). • Connection Type: **3** • Description: Any documentation. • Choose *Enter*. • Target Host: The host of your partner group. • System Number: The system number of your partner group. On the *Logon/Security* tab page, enter the logon information that you received from your partner group. Choose *Save*. Choose *Test Connection*. If the connection test fails, check the data for *Target Host* and *System Number* with your partner group. Choose **F3** to go back a step, and choose *Create* again. Call the second RFC connection <*SID*>*_ANALYSIS* (replace <*SID*> with the <*SID*> of your partner group's system). Otherwise, enter the same data as for the RFC connection <*SID*>*_DATA*, with one exception: On the *Logon/Security* tab page, select *Current User* instead of entering the logon information. Choose *Save*. Perform a connection test again. Return to transaction *RZ21* by choosing **F3** twice. In the Da*ta Collection* field, enter the RFC connection **<SID>_DATA**. In the *Analysis Method* field, enter the RFC connection **<SID>_ANALYSIS**. Choose *Save*. The message y<*SID*> *was entered in ALSYSTEMS* informs you that the registration of the SAP system was successful. You can not yet see any data for the system of your partner group, as all monitors delivered by SAP display only local data.

3	**Create a properties variant**
3.1	**Create your own properties variant, *TEST*, in your SAP system.** **Activate your properties variant.** Call the configuration transaction for the CCMS Alert Monitor (*Tools* → *CCMS* → *Configuration* → *Alert Monitor*, transaction *RZ21*). Choose *Properties* → *Variants* → *Create*. Enter *TEST* as the variant name and enter a short description. Choose *Save*. Choose *Properties* → *Variants* → *Activate*. Select your variant *TEST* and choose *Enter*. The *TEST* variant is displayed as the active variant in the initial screen of transaction *RZ21*.
4	**Create a monitor set**
4.1	**Create your own monitor set, *System Monitoring*.** Call the CCMS Alert Monitor (*Tools* → *CCMS* → *Control/Monitoring* → *Alert Monitor*, transaction *RZ20*). Activate the maintenance function, by choosing *Extras* → *Activate Maintenance Function*. Choose *Create*. *New Monitor Set* is already selected. Choose *Copy*. Enter the name `System Monitoring` for your monitor set. Maintain the attributes of your monitor set as you wish. Choose *Copy*. Your monitor set is displayed under *My Worklist*. You can now create new monitors in this set.
5	**Create a monitor**
5.1	**Create your own cross-system monitor, *Core_information* that displays the most important system monitoring data. First consider which information is important for monitoring from your point of view. Remember that you should not display too many values for each SAP system.** Your new monitor, *Core_information*, should contain the most important monitoring data for your system landscape. It could, for example, contain the following data: • Status of the last DB backup • Status of the last DB log backup • Free space in the log file system (DB-dependent) • DB errors • Terminated updates • Terminated ABAP programs

	• System log • Average dialog response time
5.2	**Now create the monitor *Core_information*. The monitor should, as far as possible, display the desired data for your system and your partner group’s system.** **Structure the monitor using virtual nodes.** In maintenance mode of transaction *RZ20*, place the cursor on your monitor set and choose *Create*. The system displays the currently registered SAP systems. Expand the tree and search for monitoring attributes that correspond to the data that you require. For the suggested monitor from exercise 5.1: • Status of the last DB backup: Look in the branch *<SID> - <Database Type> - Backup/Restore*. • Status of the last DB log backup: Look in the branch *<SID> - <Database Type> - Backup/Restore*. • Free space in the log file system (DB-dependent): Look in the branch *<SID> - <Instance> - OperatingSystem – Filesystems.* • DB errors: Look in the branch *<SID> - <Database Type> - Health - Errors*. • Terminated updates: Look in the branch *<SID> - <Instance> - R3Services – Update – AbapErrorinUpdate.* • Terminated ABAP programs: Look in the branch *<SID> - <Instance> - R3Abap - Shortdumps*. • System log: Look in the branch *<SID> - <Instance> - R3Syslog*. • Average dialog response time: Look in the branch *<SID> - <Instance> - R3Services – Dialog – ResponseTime.* Select the MTEs that you require. Choose *Save*. Enter **`Core_information`** as the name of your monitor. Open your monitor by double clicking it. The desired data is displayed, but the monitor is unclear without virtual nodes. Choose *Monitor → Change*. You can use virtual nodes to separate the data for your system and for your partner group’s system. Place the cursor on *Core_information* and choose *Create*. *Virtual node* is already selected. Choose *Continue*. Enter the SID of your system as the node name. Choose *ENTER*. The newly created virtual node is at the bottom of the list. Create another virtual node for your partner group’s system in the same way. Delete your previous selections. Expand the tree below your virtual nodes and select the desired MTEs for each SAP system. Choose *Save*. Your monitor has become significantly clearer due to the virtual nodes.

6	**Maintain threshold values**
6.1	**Open your *Core_information* monitor. Display all alerts for the entire monitor.** **Process an alert for the partner group's system, as described in exercise 1.1:** • **Start the analysis method for an alert.** • **Return to the Alert Browser and complete the alert. Does the alert still appear in the list?** **How can you display the completed alert again?** Open your *Core_information* monitor by double clicking it. Switch to the *Open Alerts* view. Double click an MTE for your partner system. All alerts in this area for your partner system are displayed in the Alert Browser. Select an alert in the list. Then choose *Start Analysis Method*. The logon screen of the partner system appears, as *Current User* is selected for the user data in the RFC connection for starting analysis methods. Log on to your partner system. In the partner system, you jump to an action that provides you with detailed information about the alert. Return to the monitor. Choose *Complete Alerts*. The alert is removed from the list. To display the alert again, choose *Show Alert History*. Your completed alert has the status *DONE*. You have just worked on a cross-system basis with the Alert Monitor.
6.2	**Maintain the threshold values for a monitoring attribute in your monitor. To do this, find a monitoring attribute from your SAP system, for which you can maintain the thresholds for:** • **Green to yellow** • **Green to red** • **Red to yellow** • **Yellow to green** **Change these threshold values and save them.** **(Note: These threshold values can only be specified for performance monitoring attributes. There are two other monitoring attribute types, for which threshold values are specified in a different way.)** Show a description of the symbols that are used in the monitor by choosing *Extras* → *Legend*. The symbol for performance attributes is a curve. Search for a performance attribute for **your** SAP system in your monitor (such as the average dialog response time). Place the cursor on a monitoring attribute and choose *Properties*. The current threshold values are displayed on the *Performance Attribute* tab page. Do you consider the threshold values to be appropriate? Choose *Display* <-> *Change* and change the threshold values.

	Choose *Save*. The threshold values are successfully adjusted and are stored in your properties variant. We recommend that you perform this check for all monitoring attributes for your system that are important for you. To activate the threshold values in other systems, you can transport your properties variant to these systems.
7	**Manual switch of properties variants**
7.1	**Activate the *SAP-DEFAULT* properties variant in transaction *RZ21*. What is the threshold value for the MTE that you set in exercise 6.2?** Call the configuration transaction for the CCMS Alert Monitor (*Tools → CCMS → Configuration → Alert Monitor*, transaction *RZ21*). Choose *Properties → Variants → Activate*. Select the *SAP-DEFAULT* variant and choose *Enter*. The *SAP-DEFAULT* variant is displayed as the active variant in the initial screen of transaction *RZ21*. Now open the *Core_information* monitor in transaction *RZ20* by double clicking it. Search for the monitoring attribute for which you changed the threshold values in exercise 6.2. The threshold values are now once again set to the original values delivered by SAP, which are anchored in the *SAP-DEFAULT* properties variant. If you reactivated your *TEST* properties variant in transaction *RZ21*, the changed settings would become active again.

Introduction to System Security

9. Support Packages and Industry Solutions

10. Scheduling background tasks

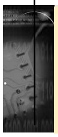
11. Printing from SAP systems

12. Basics of user administration

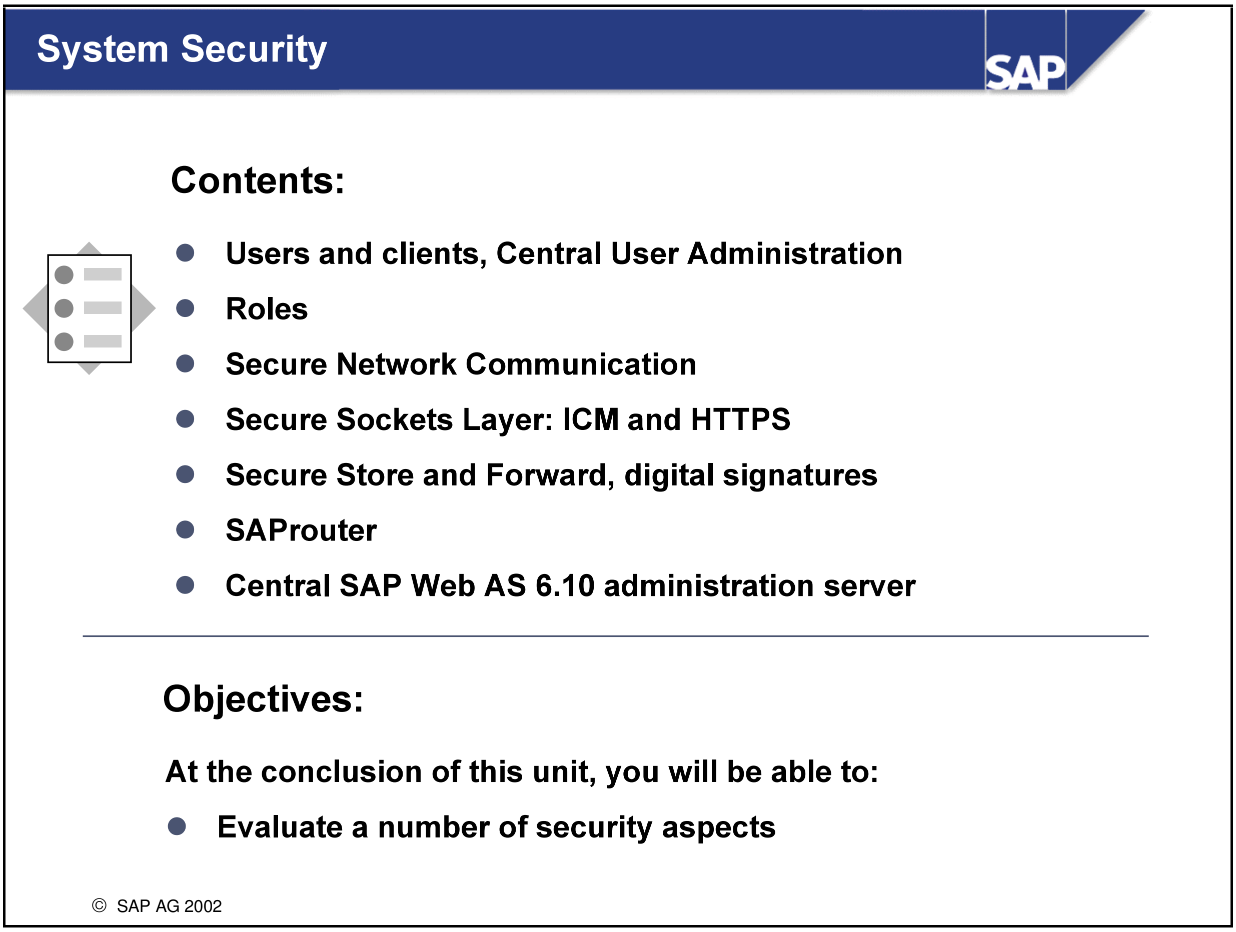
13. Remote connections

14. SAP Solution Manager

15. System monitoring



16. Introduction to system security



System Security

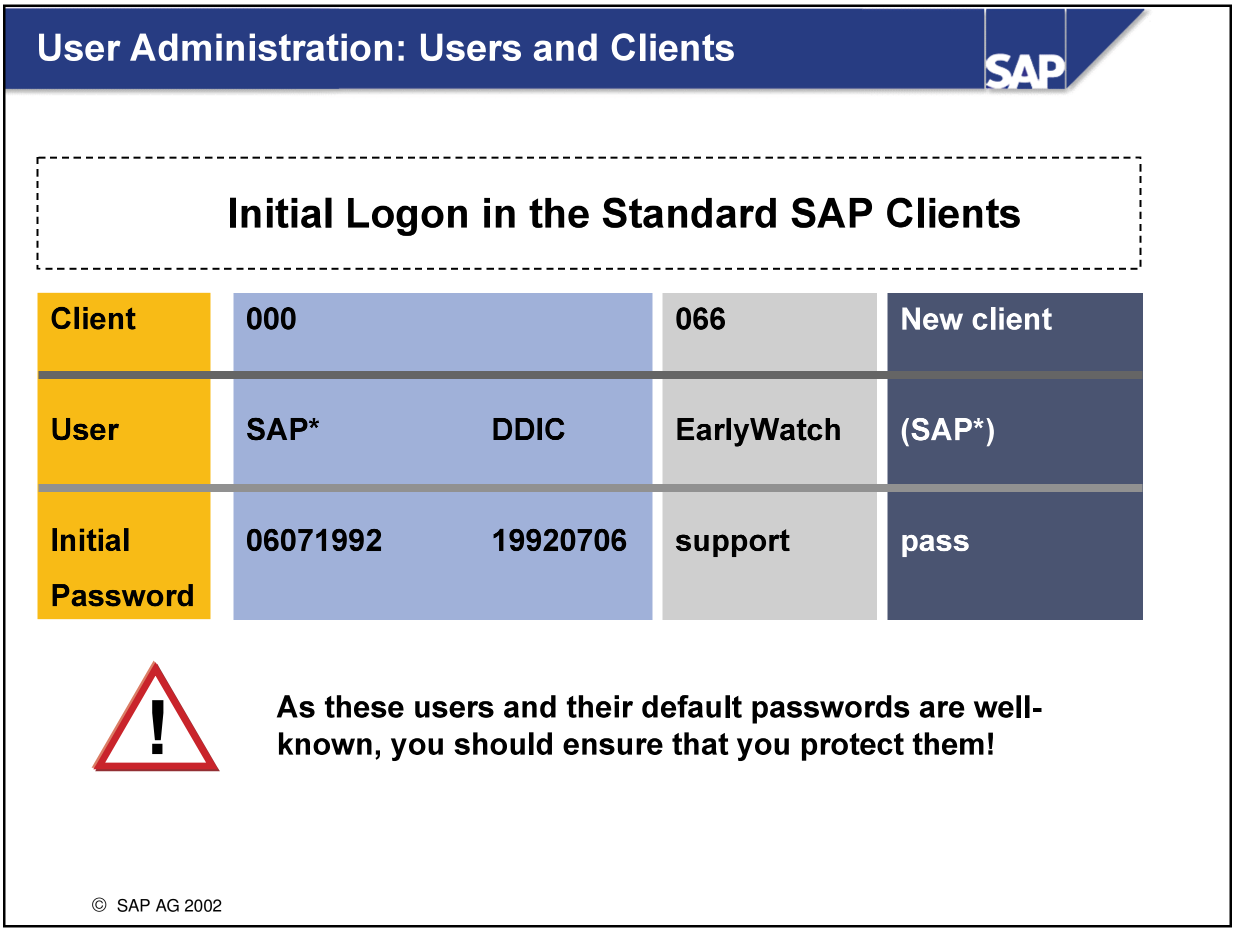
Contents:

- Users and clients, Central User Administration
- Roles
- Secure Network Communication
- Secure Sockets Layer: ICM and HTTPS
- Secure Store and Forward, digital signatures
- SAProuter
- Central SAP Web AS 6.10 administration server

Objectives:

At the conclusion of this unit, you will be able to:

- Evaluate a number of security aspects



User Administration: Users and Clients

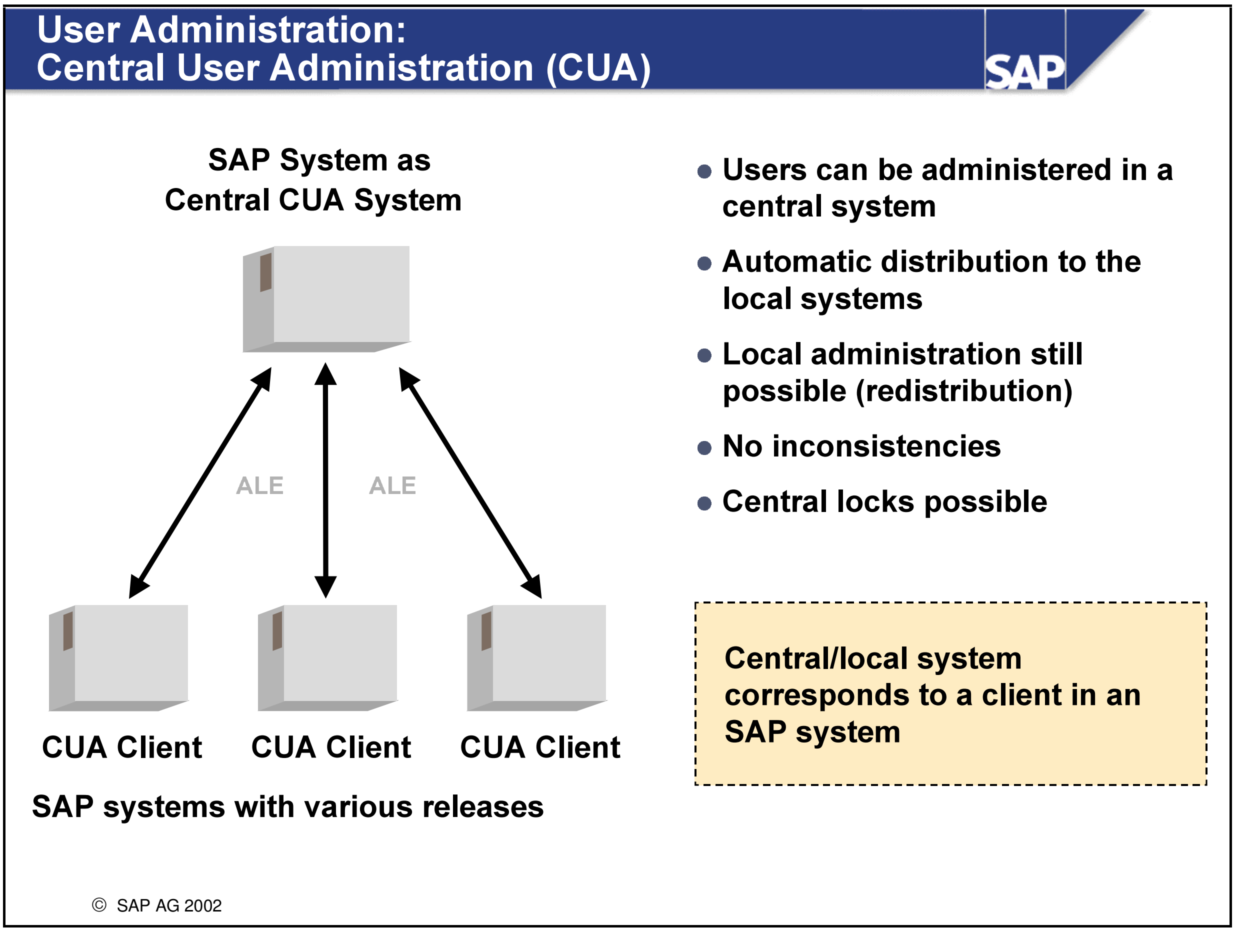
Initial Logon in the Standard SAP Clients

Client	000		066	New client
User	SAP*	DDIC	EarlyWatch	(SAP*)
Initial Password	06071992	19920706	support	pass

As these users and their default passwords are well-known, you should ensure that you protect them!

© SAP AG 2002

- Clients 000 and 066 are part of the standard SAP system.
- There are two special users in client 000:
  SAP* for initial access to the system
  DDIC for working with the Transport Management System (TMS)
- To protect SAP* and DDIC against unwanted access, you should change the initial passwords.
- Client 066 is the EarlyWatch client. You should also change the initial password for the EarlyWatch user. This user does not have any critical authorizations.
- If no SAP* user exists in a client, a mechanism coded in the kernel allows you to logon with *SAP** and the password *pass*.
  Caution: This mechanism also applies if the proper SAP* user is, for example, deleted from a client using database methods. Access to the database means access to the SAP system.
  This mechanism can be deactivated using the profile parameter ***login/no_automatic_user_sapstar***. However, it is then not possible to log on to a newly created client, for example to perform a client copy. See SAP Note 68048.
- To check the initial passwords, you can also call report RSUSR003.



User Administration: Central User Administration (CUA)

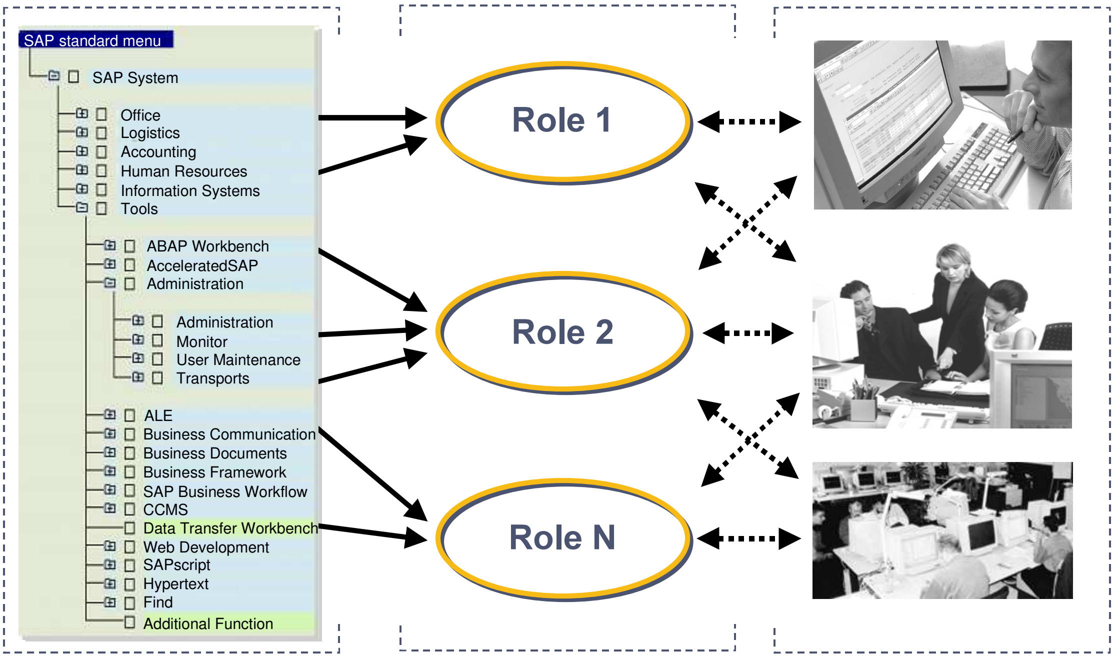
SAP System as Central CUA System
ALE
ALE
CUA Client
CUA Client
CUA Client
SAP systems with various releases

- Users can be administered in a central system
- Automatic distribution to the local systems
- Local administration still possible (redistribution)
- No inconsistencies
- Central locks possible

Central/local system corresponds to a client in an SAP system

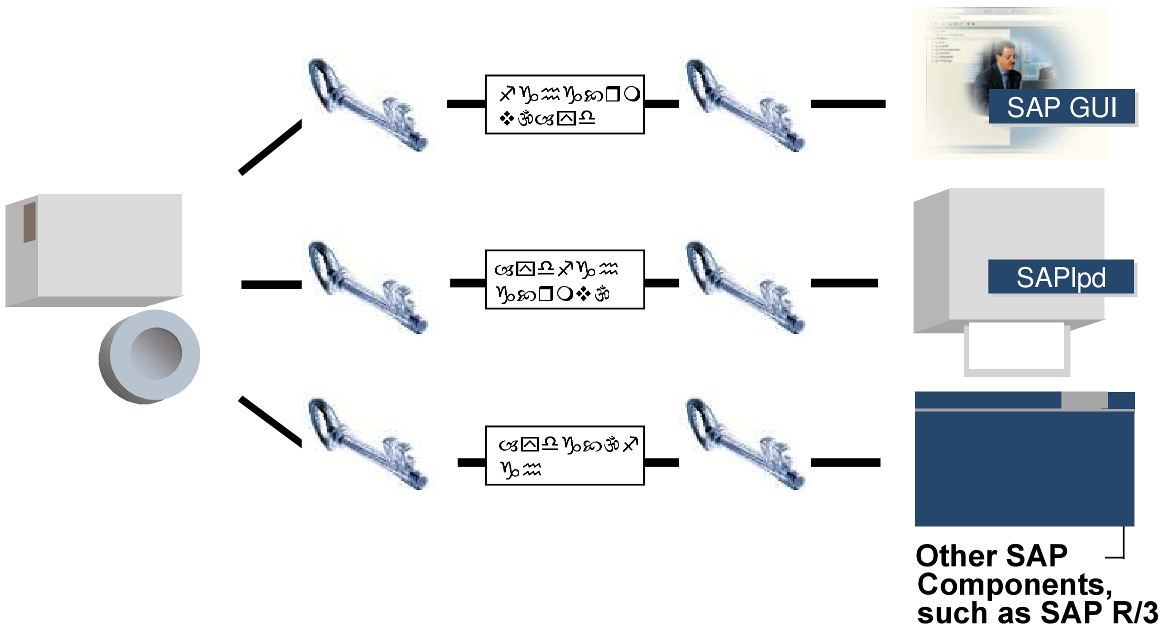
- To simplify the administration of user master records among several logical systems, you should use Central User Administration (CUA). In terms of CUA, a logical system corresponds to a client in an SAP system.
- CUA provides an overview of all users, all user groups, defined systems, and system groups, and defined roles.
- Using the CUA, you can maintain user master records from a single client, and distribute this information to all included clients of all systems. In this context, there is one logical system that controls the user master records of all logical systems.
- Reasons for using CUA:
  - Complex system landscape with multiple clients in various systems.
  - The same user works in multiple logical systems.
  - The same user name should represent the same user.
  - It would require a great effort to synchronize the user data in all included systems.

User Administration: Roles



- A role is a work center description.
- You can assign authorizations to users using role maintenance. For example, select from the SAP menu or manually insert transactions and URLs.
- Changing a role changes the authorizations of all users to whom this role is assigned.
- You must configure role maintenance before you can use it.
- For more information, see online help or the documentation *Authorizations Made Easy* from the SAP Simplification Group.
- The course CA940 also provides additional information about administering users in SAP systems.

Secure Network Communication (SNC)

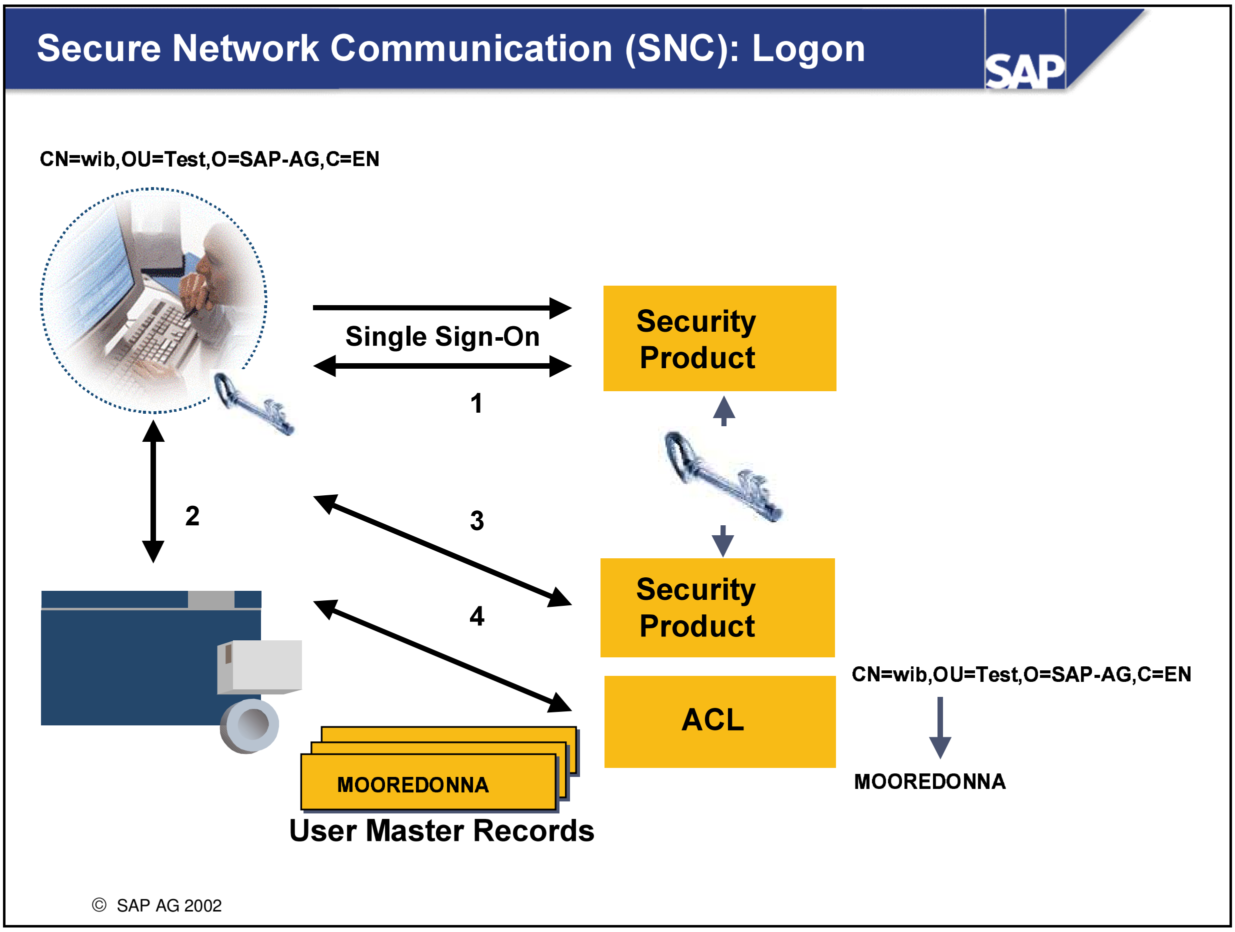


SNC allows the encryption of the DIAG and RFC protocol

- SNC is a software layer in the SAP system architecture that provides an interface to an external security product. You can increase the security of your SAP system with SNC by implementing additional security functions that are not directly provided by SAP systems (such as the use of smart cards for user authentication).

- SNC provides security at application level. This means that a secure connection is guaranteed between the components of an SAP system (for example, between the SAP GUI and the SAP application server), irrespective of the communication connection or the transport medium. You therefore have access to a secure network connection between two communication partners secured with SNC.

- There are three different protection levels for communication connections secured with SNC:
    - **Authentication only:** With authentication, only the identity of the communication partner is checked. This is the lowest protection level when using SNC. (There is no actual data security.)
    - **Integrity protection:** If you use the integrity protection, the system recognizes changes to the data that have been made during the transfer between the sender and the recipient.
    - **Confidentiality protection:** For the confidentiality protection, the transferred messages are encrypted, meaning that eavesdropping is pointless. This is the highest SNC protection level. This protection level also includes the integrity protection and authentication.



Secure Network Communication (SNC): Logon

1. The user logs on to a security product (such as Secude) using Single Sign-On.

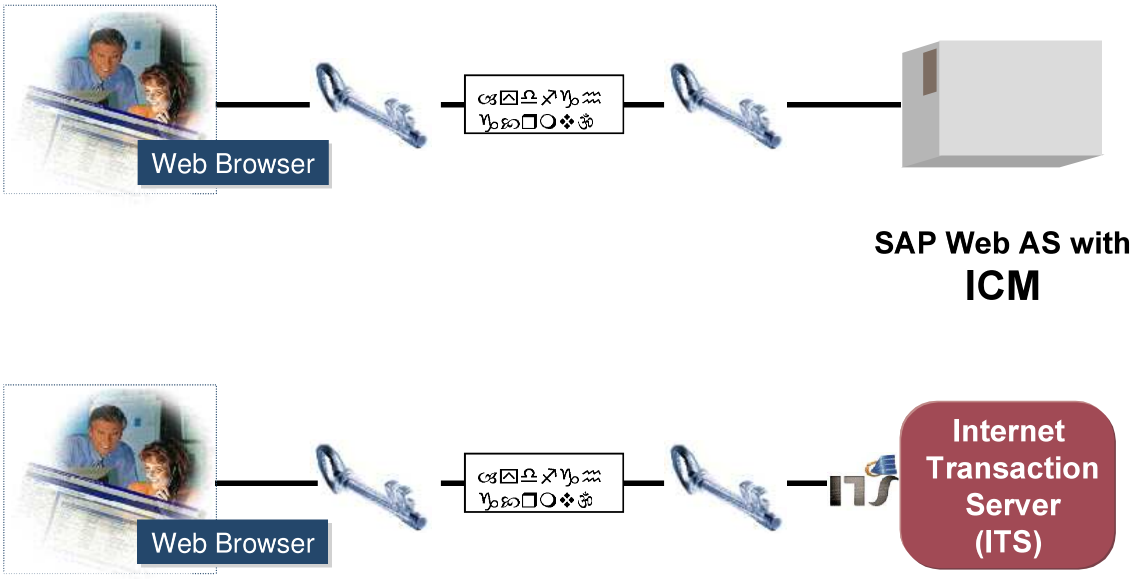
2. When the user logs on to other included systems (such as SAP R/3), the user name and password are not requested from the user.

3. Instead of this, the system communicates with the security product.

4. The logon string is triggered in the user master record using the Access Control List (ACL), allowing this user access. The two components of the security product exchange information using SNC.

- In some countries, the use of cryptography is legally controlled. If you use SNC, you should learn the effects of these laws on your applications, and ensure that you are aware of all further developments.

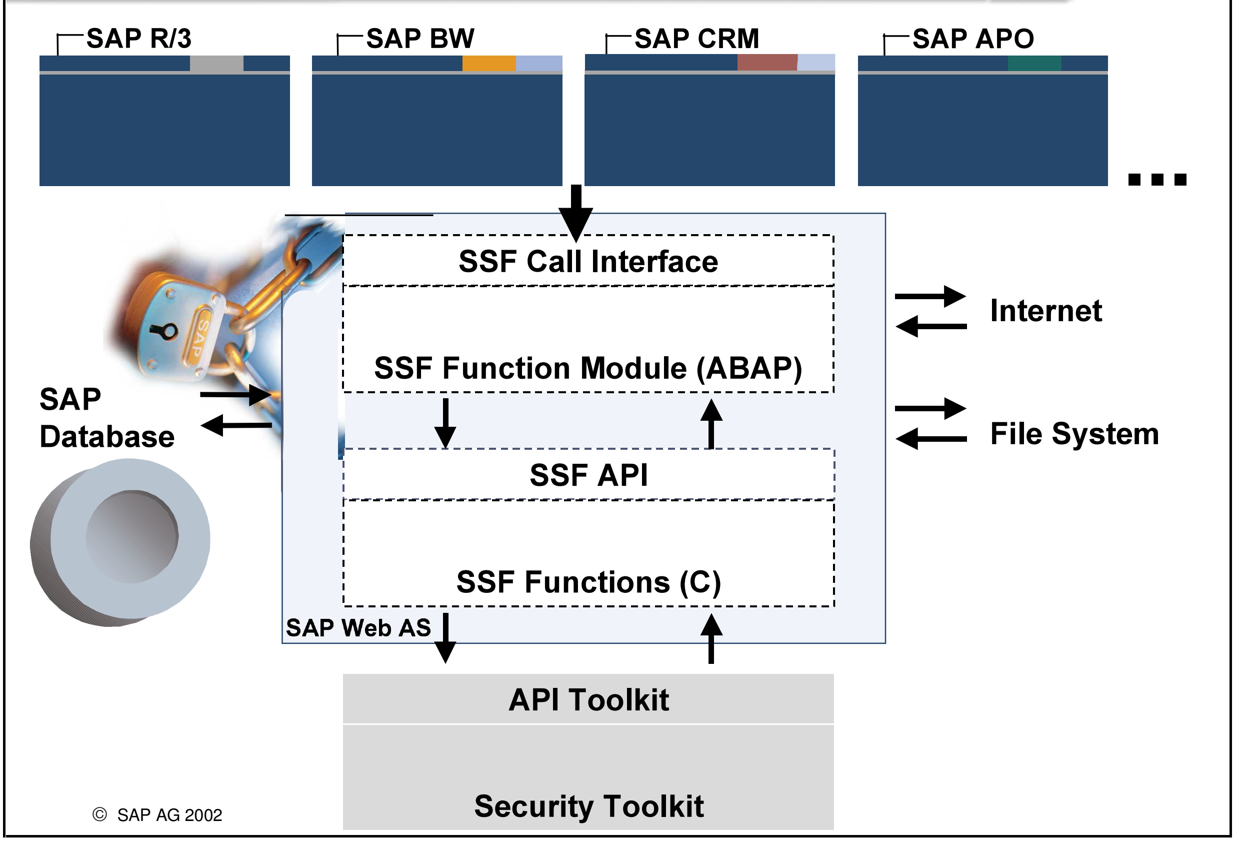
Secure Socket Layer (SSL): ICM and HTTPS



SSL allows the encryption of the HTTP protocol

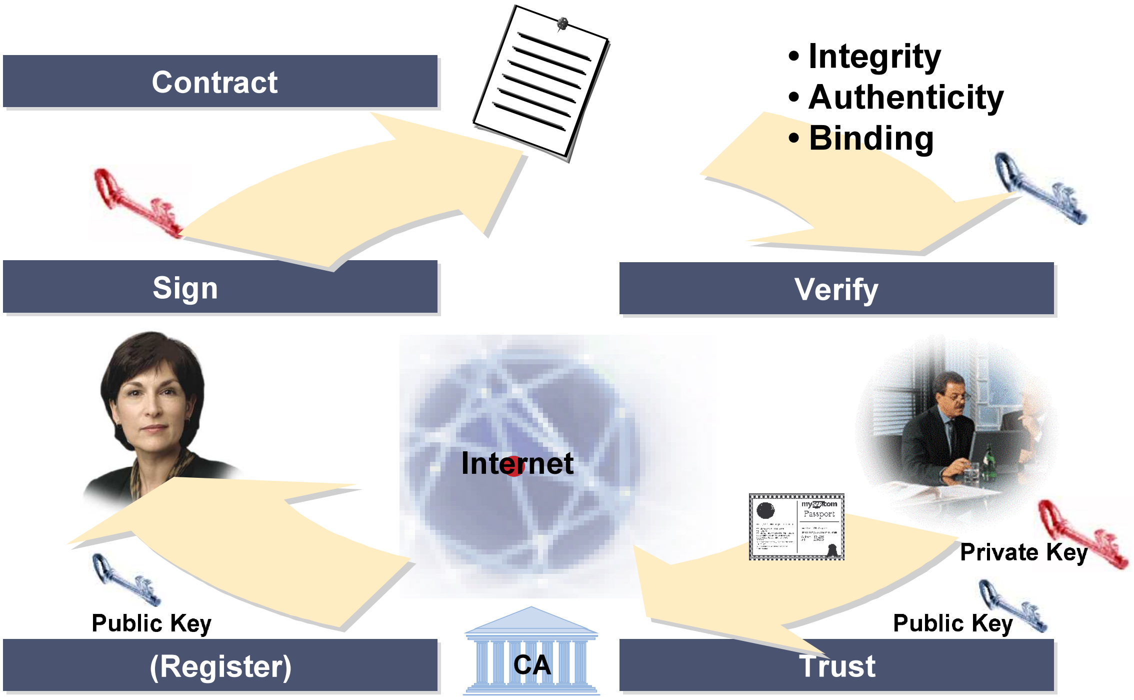
- Secure Network Communication (SNC) allows you to encrypt the DIAG and RFC protocol. Secure Sockets Layer (SSL) works in the same way for the HTTP protocol. This creates an HTTPS (“S” for secure) protocol from the HTTP protocol. In this way, it is possible to exchange confidential data (for example, over the Internet).
- Among other places, SAP uses SSL:
  - For direct communication between the SAP Web AS and the Internet. In this case, the SAP Web AS "speaks" in HTTP. This is possible with the Internet Communication Manager (ICM) component, standard as of SAP Web AS 6.10.
  - For communication with the Internet using an Internet Transaction Server (ITS). In this case, the HTTP protocol is encrypted by the W Gate of the ITS.

Secure Store and Forward (SSF)



- SSF ensures that SAP system data and documents are secure during and beyond dialog transactions:
  - Data leaves the system (electronic orders, invoices, information)
  - Data is stored in unsecured media (external databases, diskettes, archives)
  - Data is transferred using unsecured networks (Internet)
  - Data security relates to people and individuals (digital signatures, personal data)
- Aims are therefore:
  - Data security
  - Security of personal data
  - Authentication
  - Non-reproducability
- This is achieved using digital signatures and digital envelopes. Package Key Cryption Standard Number 7 (PKCS#7) is used as the standard format.

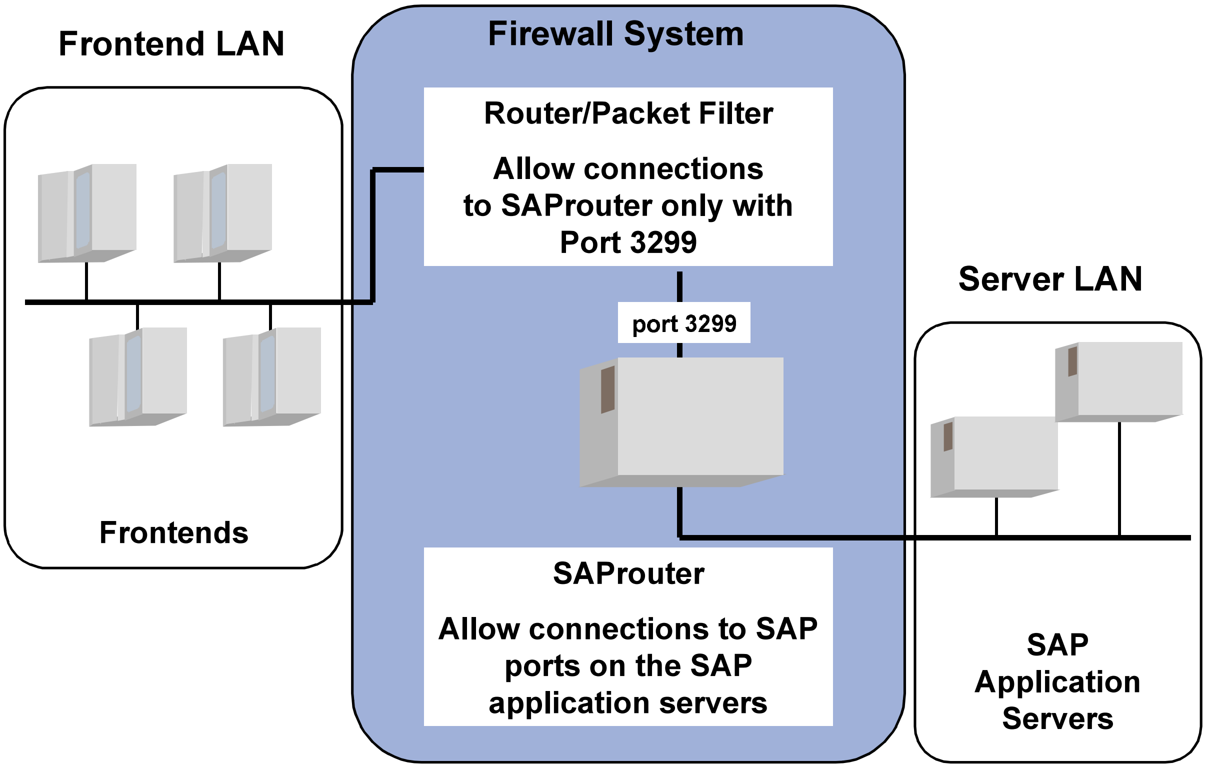
Digital Signatures and Envelopes



CA = Certification Authority

- A Certification Authority (CA) issues a certificate and digitizes it. This certificate contains, among other things, the name of the holder, the name of the issuer, a validity period, and the public key. The certificate can be passed on as desired. There is a private key that matches the public key, which only the holder knows. The private key cannot be calculated from the public key.
- People that do not know each other directly (for example, in the case of a query over the Internet) can communicate authentically with each other with the help of the CA.
- SAP uses standard technology for the implementation of digital signatures. Digitally signed documents are created as PKCS#7 packages.
- Possible applications: Orders (B2C, B2B), applications (Public Sector), cross-system processes, and so on.
- ABAP interface for digital signatures: Secure Store and Forward (SSF).
- Signatures can by made by application servers or by users with the SAP GUI or in a Browser.
- For more information, see the SAP Service Marketplace with the Quick Link */security*.

SAProuter



Frontend LAN

Frontends

Firewall System

Router/Packet Filter

Allow connections to SAProuter only with Port 3299

port 3299

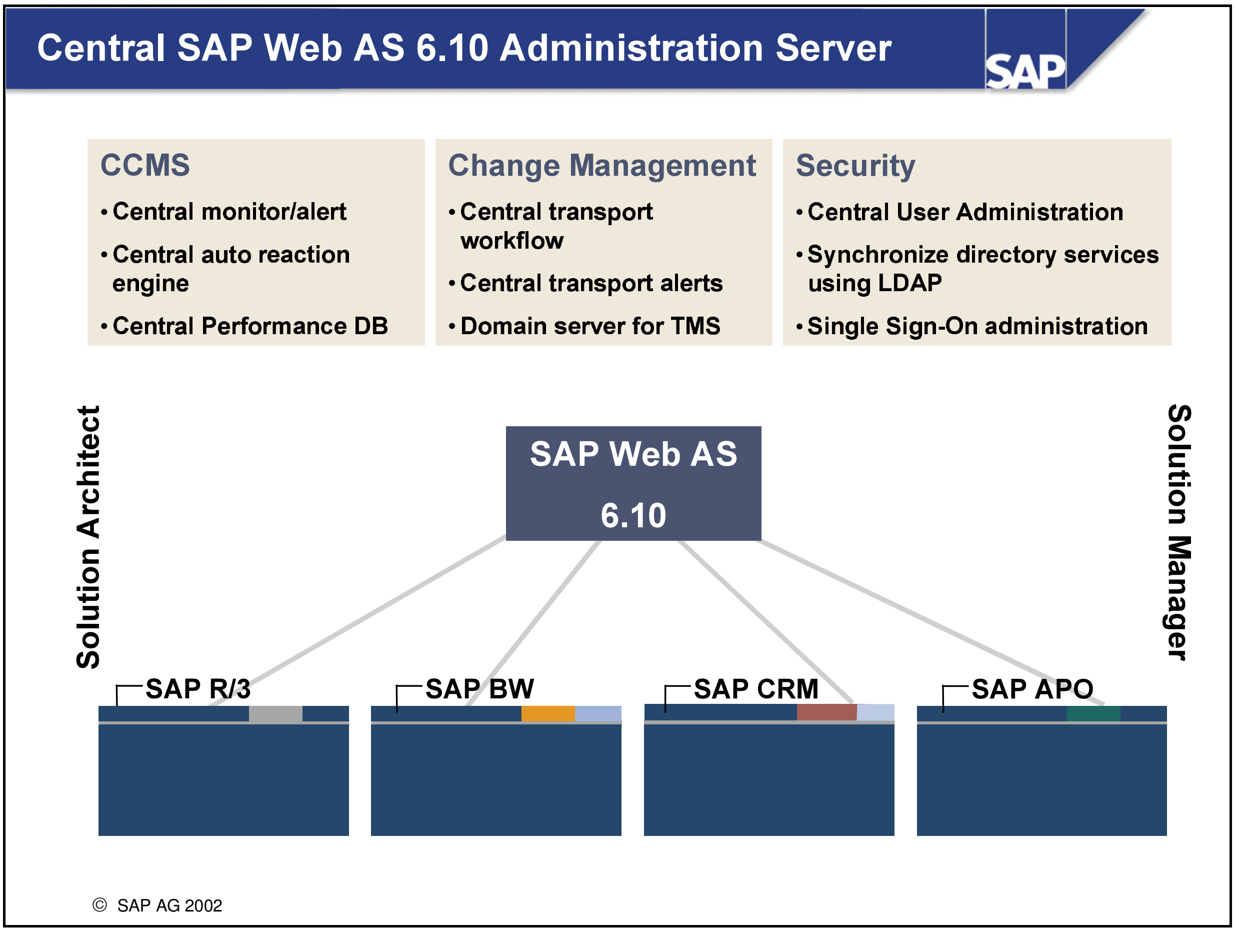
SAProuter

Allow connections to SAP ports on the SAP application servers

Server LAN

SAP Application Servers

- SAProuter is an SAP program for forwarding SAP system connections through firewalls. The SAProuter extends the firewall, but does **not** replace it. We recommend that you use SAProuter together with a firewall. Caution: A single SAProuter will not protect your SAP system network. You must use a SAProuter for the SAP Remote Services (SAPNet - R/3 Frontend).
- You can also use SAProuter to:
  - Control and log connections to your SAP system.
  - Create an indirect connection if the programs involved in the connection cannot communicate directly due to the network configuration.
  - Resolve address conflicts if unregistered IP addresses are used.
  - Improve network security, by:
    - Protecting your SAProuter from unauthorized external access.
    - Only allowing access from certain SAProuters.
    - Only allowing secured connections from a secure authenticated partner (SNC).
  - Improve the performance and stability by reducing the load of the SAP system in a LAN for communication with a WAN.
- If you use SAProuter, you only need to open one port on the firewall for a connection with the port on the server on which SAProuter is running. All SAP GUI, SAPlpd, and RFC connections must pass this port (default 3299). For more detailed information about the use of SAProuter, see SAP Note 30289.



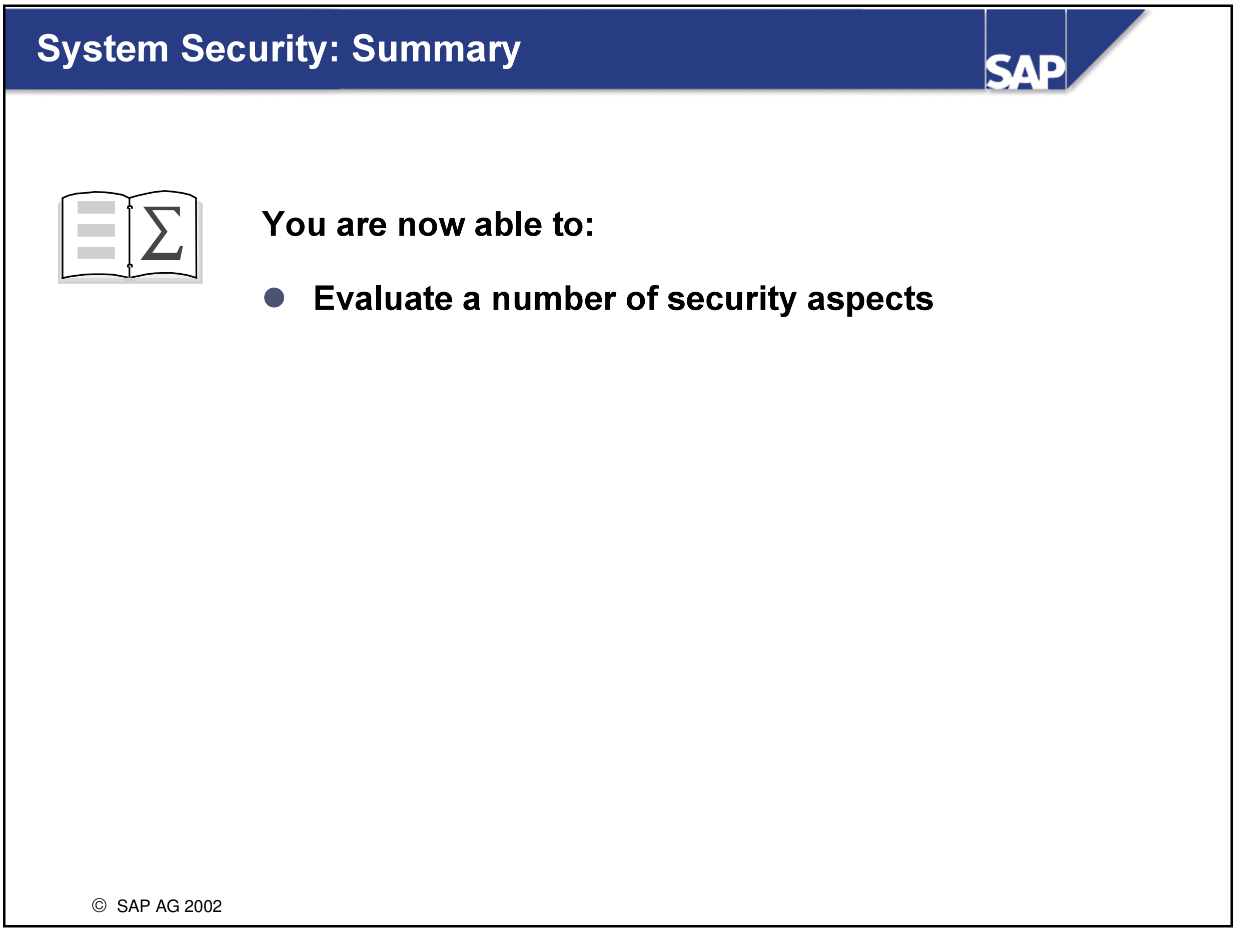
Central SAP Web AS 6.10 Administration Server

CCMS
- Central monitor/alert
- Central auto reaction engine
- Central Performance DB

Change Management
- Central transport workflow
- Central transport alerts
- Domain server for TMS

Security
- Central User Administration
- Synchronize directory services using LDAP
- Single Sign-On administration

- SAP recommends that you set up a SAP Web AS 6.10 for every mySAP.com system landscape for monitoring, alerts, transport organization, and Central User Administration (CUA).



System Security: Summary

You are now able to:

- Evaluate a number of security aspects

© SAP AG 2002