Corso ManageEngine OpManager

Sommario

[Lezione 1 (23/03/2020) 2](#_Toc38897211)

[Lezione 2 (31/03/2020) 4](#_Toc38897212)

[Lezione 3 (06/04/2020) 5](#_Toc38897213)

[Lezione 4 (14/04/2020) 7](#_Toc38897214)

[Netflow 7](#_Toc38897215)

[Network Configuration Manager 8](#_Toc38897216)

[Firewall Analyzer 8](#_Toc38897217)

[OpUtils 9](#_Toc38897218)

[ApplicationManager 9](#_Toc38897219)

[Appunti e domande 10](#_Toc38897220)

[PREREQUISITI 10](#_Toc38897221)

**Link lezioni:**

Sessione 4: [https://register.gotowebinar.com/register/7159261462715605003](https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Fregister.gotowebinar.com%2Fregister%2F7159261462715605003&data=02%7C01%7Cmarketing%40bludis.it%7C97fd1c3dd505486edb7708d7db021c34%7Cc9cccb0b0da248079f9334d70e5f4e9f%7C1%7C0%7C637218674454007282&sdata=acdGnGtvH1ydtWeszkurfA%2B6b3fSaJkQDzGRAd6vgtI%3D&reserved=0)

Sessione 6: https://register.gotowebinar.com/recording/viewRecording/4506386195496774155/4356490875658259472/federico.coppola@connectspa.it?registrantKey=1266641099404592397&type=ATTENDEEEMAILRECORDINGLINK

**LINK UTILI:**

* <https://www.manageengine.com/network-monitoring/network-performance-management.html>
* <https://www.manageengine.com/network-monitoring/help/index.html>

# Lezione 1 (23/03/2020)

**Esistono varie versioni di OpManager.**Professional ed Enterprise 🡪 cambia architettura e pacchetti che si possono scaricare e installare

Professional singola installazione (solo una macchina che si dedica al monitoring)  
Enterprise adatta ad aziende con realtà medio-grandi (varie macchine installate che si occupano del monitoring e report). Ci sarà una macchina **central** che si occupa di inviare report e centralizzare le informazioni!

**Professional fino a 1000 device, oltre è necessaria la versione Enterprise**

Le macchine periferiche (**PROB**) inviano info alla macchina centrale tramite http o https  
Si consigliano almeno 16gb di ram per il corretto funzionamento.  
Durante l’installazione ci viene data la possibilità di scelta del database.  
**PostgreSQL è quello incluso ed installato in modo automatizzato (consigliato)**  
In alternativa bisogna installare Microsoft SQL

Ci sono anche client per Android e iPhone!

**OpManager si occupa di monitoraggio dei dispositivi (di rete ad esempio)  
ICMP e SNMP 🡪 dispositivi di rete**

Si possono configurare monitor IP SLA (WAN, VoIP, Video) per device Cisco

Si possono monitorare server (Windows con librerie WMI e questo implica che sia installato su macchina Windows OS) fisici o virtuali (VMware, Citrix, Microsoft)

Si possono creare allarmi e reporting (oltre 100 report).  
Vari tool per infrastruttura.  
  
Monitoring dedicato per device di storage (monitor particolari, non solo classico SNMP) 🡪 licenze extra

Utenza di default è admin/admin subito dopo installazione

Settings > General settings si possono configurare impostazioni di base come Mail e Utenti (anche integrando Active Directory), porta per accedere in HTTP…

Nel sottomenu “System Settings” si abilitano i componenti extra attivati dopo aver acquistata la licenza.

**L’utenza può essere Operatore o Amministratore; si può decidere cosa può essere visto dall’utente creato**

**Security Settings***SSL Configuration* si può accendere il protocollo HTTPS, usando self-signed certificate o con certificato acquistato

**Creare credenziali per accedere agli host (utente, SNMP community…) prima di aggiungerli sotto monitoring. In questo modo discovery e aggiunta device più velocemente.**

Per aggiungere i device bisogna scegliere il menù riguardante la tipologia poiché OpManager gestisce in modo dedicato la gestione degli storage e virtualizzazione!

Si possono creare discovery profile ovvero specificare intere subnet o range di IP da mettere sotto scansione per aggiungere host in automatico (usando le credenziali precedentemente indicate)

**Ci sono dei template dedicati ai device. I template servono per il monitoraggio.**

Tab Monitoring (nel menù settings) si occupa degli indici di performance e applicazioni.

In produzione è consigliato l’utilizzo di Microsoft SQL (non la versione Express)

# Lezione 2 (31/03/2020)

È possibile personalizzare i “Device Template”  
I template si “possono migliorare” con custom settings.

**Performance** 🡪 Selezionando un monitor (sono i controlli, ad esempio l’uso di CPU…) e si possono modificare i suoi valori come il timer di checkup etc...

Inoltre, è possibile aggiungere nuovi monitor custom selezionando il pulsante “Add Monitor”  
In fase di creazione si sceglie se usa SNMP o WMI (Windows Server).  
**SNMP** 🡪 Scelgo il device (in modo da verificare la bontà), imposto OID oppure upload MIB.  
Tramite il pulsante “Test OID” vediamo subito se è OK

Le MIB si possono impostare tramite **Settings > Tool > MIB Browser**  
**RFC1213 è l’elenco dei MIB standard dei Network Device**

**Application Monitor** 🡪 ci sono alcuni monitor già presenti soprattutto per Server sui quali ci sono varie app che lui sa “gestire”.  
Direttamente da OpManager è possibile gestire qualcosa in modo basilare, altrimenti prodotto dedicato extra.  
I prodotti che sa gestire sono quelli di Microsoft (Active Directory ed Exchange)

**Windows Services** 🡪 servizi di base di Windows (sempre tramite WMI)

**WMware events**

**Processes** 🡪 processi veri e propri di sistema (es. explorer.exe)  
Quando si creano si indica il nome del processo, path e threshold

**Files** e **Cartelle (Folders)** 🡪 monitoring file e cartelle (sempre di Windows OS)

**Services Monitor** 🡪 servizi di rete come DNS, HTTPS…. Ed è possibile aggiungere porte extra

**URL** 🡪 raggiungibilità di URL HTTP/HTTPS. Si possono anche impostare credenziali per accedere all’URL.  
 Si possono importare anche molteplici URL in CSV (molto comodo!)

**SNMP TRAP PROCESSOR 🡪** Permette di monitorare ricevendo sulla porta UDP-162 le trap inviate dai device. OpManager è in grado di ricevere SNMP! Le trap ricevute vengono automaticamente riconosciute e quindi si capisce quale evento è accaduto.

Spesso ormai molti vendor forniscono anche le MIB riguardanti le TRAP ricevute.  
**RFC1215-TRAP** 🡪 per device di networking

**Syslog** 🡪 regole riguardante i syslog  
**Si può eseguire il forwarding dei logs o SNMP verso un SIEM ad esempio**

**Script Templates** 🡪 si possono creare, importare script

**Gli ambienti WMware sono monitorati direttamente da API e non tramite SNMP**

**URL Templates** 🡪 si monitorano altri aspetti degli URL

**IPSLA** 🡪 monitor dedicato al mondo networking.  
IPSLA è un protocollo nativo di Cisco monitora i link Dati, VoIP, Video. **Bisogna avere community SNMP WRITE, non basta di tipo READ-ONLY**

I monitor IPSLA si configurano tramite il menu *Network > IPSLA*

**Monitor Settings** 🡪 si stabiliscono politiche generali riguardanti il monitoring come se usare IP o DNS, abilitare HW Monitoring e relativo polling interval…

**Grouping dei devices** permette di creare gruppi di device da *Settings > Configuration > Groups*

È possibile definire “health” del gruppo. Utile se ci sono più host in un gruppo e questi host non necessariamente devono essere tutti UP affinché tale servizio sia operativo.

Vendor template contiene gli OID dei vendor (Cisco, HP, Dell, Fortinet…).

Il Device Template viene applicato al dispositivo una volta riconosciuto.  
*Show Dial* ci permette di vedere quali info si vedono nella pagina principale del device.  
Al template si associano i Monitor.

Le personalizzazioni si possono fare a livello di template o sul device.   
Consigliato farlo a livello di template, eccetto per casi particolari in modo esclusivo dei device.

Si può impostare il timer di polling per le singole interfacce e applicare relativi threshold.

Nel menu **configuration > Device Downtime schedules** possiamo impostare il periodo in cui ci saranno disservizi ad esempio per maintenance e quindi non ci deve inviare alert via mail.  
Sì può ripetere in automatico (giornalmente…) e

limitarlo ad alcuni host (basandosi su gruppi, categorie…)

# Lezione 3 (06/04/2020)

Nella sezione degli allarmi (Alarm > Active alarms) è presente un pollice verde sulla destra che i permette di determinare l’ACK del trigger. In questo modo comunico che il problema è preso in carico.

Tutti gli allarmi dello stesso tipo sono raccolti nella stessa pagina  
È possibile effettuare **Clear** dell’allarme (forzo la chiusura)

**Gli allarmi possono essere anche creati da altre fonti (provengono da Event Log, Syslog…)  
Queste sorgenti sono configurate in Settings > Monitoring**

**Se OpManager conosce OID crea automaticamente allarme (TRAP)  
Se OpManager non conosce saranno raggruppate in *Alarm > Unsolicited Trap***

La pagina principale della macchina sotto monitoring viene detta “pagina di snapshot”

È possibile associare un monitor dal singolo HOST tramite il menu “Monitors” presente nella pagina principale del device scelto, selezionando la tipologia (Performance, Event…) e poi associandolo tramite il pulsante verde “Actions”

In **Configuration > Alarm escalation rule** 🡪 creare delle regole per fare in modo che l’allarme abbia una escalation verso un livello di supporto superiore.

**Downtime schedulato** 🡪 il non generare allarme durante un periodo specifico  
Il downtime può essere schedulato o one-shot

**Gli allarmi si possono notificare in vari modi e ci sono vari tipi di notifiche (Settings > Notifications).**Si possono inviare mail, SMS ma anche eseguire comandi…

**Creazione notifica e-mail:**

1. scegliere tipologia (e-mail…)
2. scegliere il criterio (soglie, eventi HW…) e il livello di criticità
3. selezionare i device coinvolti (host sui quali si applica la regola di notifica degli eventi)
4. schedulazione (h24, solo alcuni giorni…), delay trigger, ricorrenze
5. Dare un nome al profilo e salvare!

Per usare la chat è necessaria l’integrazione con Slack, mentre per il ticketing è ServiceDesk Plus e ServiceNow

Si possono inoltrare ad un syslog specificando IP syslog server e porta; si possono inoltrare le trap ricevute verso altre destinazioni.

**WorkFlow** 🡪 avviene una azione automatica gestita dal sistema.  
Può iniziare in base ad un allarme o un evento pianificato.  
Si crea tramite drag and drop e viene configurato in base alle nostre esigenze  
Si applica alla tipologia di device.  
Infine si scelgono i trigger che lo scatenano oppure si schedula.

I workflow si possono esportare e sono dei semplici file XML.  
Si creano senza codice, è tutto grafico

Si possono integrare API e Workflow di OpManager

# Lezione 4 (14/04/2020)

**Netflow, Firewall Analyzer e OpUtils** si attiva con un semplice click (questione di licenze)

**Application Manager** 🡪 plugin da installare e appesantisce il server (valutare bene!)

Si consiglia di installarlo singolarmente su una VM dedicata e poi integrare la soluzione.  
Application Manager è la soluzione completa al monitoraggio applicativo proattivo.

Nella schermata relativa all’account si vede lo stato della licenza.

Per attivare una licenza (e quindi una di queste funzioni aggiuntive) bisogna:

1. Caricare il file di licenza tramite il menu del profilo (in alto a Destra)
2. Settings > General Settings > System Settings
3. Scorrere in fondo alla pagina e “selezionare” le funzioni che vogliamo attivare (grazie alla licenza inserita precedentemente)

## Netflow

NetFlow analizza device di Layer3 (ROUTER) ed effettua un export dei flussi.  
Tutti i vendor maggiori sono compatibili con questa funzione.  
La configurazione va fatta solo per i device da cui vogliamo esportare questi dati.  
Genera molto traffico e pesantezza per essere elaborata dai server.

Suggerito attivarlo solo in caso di troubleshooting!

NetFlow Analyzer ha una sua GUI dedicata.

Tramite questa funzione si può determinare gli usi di banda, gli utenti e applicativi in uso, attacchi basati su Zero-Day!

Si può integrare NCM in NetFlow senza OpManager.  
DPI 🡪 portare alla vista i tipi di latenza (applicativo e network)

Nel Menù “Inventory” ci sono i device che esportano i dati verso il server stesso.  
Ci sono grafici interattivi attraverso i quali possiamo analizzare le info.

Dal menù “Traffic” si possono configurare gli allarmi ed ottenere export in CVS o PDF (volume di traffico in Input e Output)

Dal menù “application” 🡪 studia il pacchetto e dice quale è l’applicativo interessato. In questo modo ci dice il traffico usato dagli applicativi e ci comunica anche le porte TCP/UDP usate

Dal menu “attacks” 🡪 attacchi o traffico che lui non vede “regolare”

**NetFlow è già incluso nel pacchetto di OpManager, bisogna solo “accenderla” grazie opportuna licenza**

**Sì può accedere direttamente da OpManager tramite Network > Flow Analysis**

**NetFlow permette di “monitorare” anche il WIFI.**La licenza varia in base al numero di Access Point da monitorare (tramite menù WLC)

Si può vedere quanti client ci sono per ogni AP, i SSID che convogliano più traffico e gli applicativi, QOS

## Network Configuration Manager

La sua funzione principale è il backup della configurazione dei device di rete

Telnet, SSH e poi editare/modificare config in questo modo.

Quando vede una modifica nelle configurazioni del device monitorato (il device deve essere monitorato) la salva nuovamente in un DB cifrato.

Si possono configurare i **Change Manangement** 🡪 si propongono modifiche e flussi di verifiche delle modifiche, ed eventuale modifica viene eseguita sui dispositivi

Verifica anche i firmware presenti e compliance dei device

I backup si basano su template che comprendono un set di comandi utile per vedere la config e poi salvarla.

Si possono inviare “pezzettini” di configurazione detti “ConfigLet”

Tramite il sottomenu “Rules” di “Compliance” si possono creare delle regole custom

**Si può gestire flusso di approvazione delle richieste in “Change Management” e poi approvarle dal manager dell’apparato.**

I template si possono modificare dal menu “Device Management”

Ha anche lui la reportistica. In modo particolare si distingue in quanto ha una sezione di report dedicata solo a End Of Life (EOL) e End Of Support (EOF)!

Il DB del server deve accedere ad Internet per fare i check di versione

## Firewall Analyzer

Il Firewall Analyzer si occupa di Firewall, si occupa di tutta la parte funzionale del firewall stesso:

* Cosa succede sulle regole
* Come si comportano le regole e il dato
* Come ottimizzare il firewall

Il “**rule management**” è il cuore del prodotto.  
Statistiche sulle regole (quelle con più match, regole ANY, regole che non effettuano match…)

Se seguiamo i consigli dello strumento possiamo ottimizzare il numero di regole.

**Rule Cleanup** 🡪 vedere regole che non vengono usate negli ultimi XXX giorni

Verifica interfacce e oggetti non usati.

**Rule Reorder** 🡪 in base al traffico del firewall ci dà un consiglio di come riordinare le regole nel firewall per ottimizzare le performance del firewall stesso

**Rule Impact** 🡪 simula funzionamento policy firewall senza causare disservizi

I firewall supportati sono quelli dei maggiori vendor (Cisco ASA, Fortinet, PaloAlto…)

**Rule Administration** 🡪 permette di creare policy da Firewall Analyzer

**Compliance** 🡪 verifica se il firewall lo è ed eventualmente come correggere

Firewall Analyzer permette di avere report su VPN tramite il menu Reports.  
Le VPN solitamente sono gestite da firewall

## OpUtils

OpUtils è IPAM di ManageEngine.

Switch Port Mapper   
Si vede quali porte sono impegante da ciascuno switch con info legate al dispositivo  
(come MAC-ADDRESS)

OpUtils non ha versione enterprise

## ApplicationManager

È un applicativo totalmente differente poiché non viene monitoraggio a livello HW o Servizio, ma in questo caso è un monitoraggio applicativo.

È un applicativo agent less.  
Servono utenze di servizio dove vogliamo monitorare e verrà quindi poi creato un monitor di quello che avviene

**Consigliato installarlo su server dedicato**

Le licenze si basano sul numero di Monitor

# Appunti e domande

Parent monitor 🡪 se il device padre è down quello che dipende da lui viene messo in “Not Monitor”

Alarm escalation profile Default 🡪 3 ore

SNMP Timeout for data collection può essere editato con **NMSProcessesBe.conf**

Seed switch è il core switch

**OpStore si attiva come Storage Monitoring (da System Settings)**

Quanti byte usa il ping? 32 byte

Che cosa è utilizzato per verificare raggiungibilità di un host? PING/ICMP

Quale network device lavora nel layer fisico? HUB

Quale protocollo di trasporto per Best Effort? UDP

Possibile aggiungere widget nella dashboard? Yes

Device di rete che permette di connettere parte radio a quella fisica? Access Point

È usato per convertire IP address in indirizzo fisico? ARP

Se URL è down quale sarà l’allarme? “Service Down”

Memory Balloon non viene monitorata dal menu snapshot su ESX Server

Snapshot page è la pagina principale del device

SNMP, NetFlow, IPFIX per monitorare la banda

Service monitor non per forza ha bisogno di WMI

## PREREQUISITI

* SNMP GET e TRAP da vedere
* PDU
* SNMP WALK
* Basi di IPv4 e IPv6

# Altre note e appunti

La configurazione delle dipendenze previene il controllo dello stato di dispositivi che dipendono dal nodo in questione.

Bisogna associare un Template al Monitor affinché sia applicato ai device!

OpManager tramite sysOID (protocollo SNMP) riesce a catalogare il device al suo rispettivo template.  
È una procedura automatica e può essere modificato il template associato.  
È possibile associare i Monitor ai template. In questo modo al device a cui viene associato un template viene anche già associato un Monitor.

**Associare manualmente template a device:** <https://www.manageengine.com/network-monitoring/help/associate-device-template.html>  
Una possibile strada è: **Settings → Configuration → Device Template**

**Rearm Value 🡪 il valore rearm è la soglia sotto la quale la situazione torna alla normalità**

Le soglie di allerta si possono configurare sia a livello singolo device, che a livello di template (si applica a tutti i device che hanno il template!)

WMI permette di monitorare i servizi di Windows OS

**ASSOCIARE WINDOW SERVICES TEMPLATE TO MONITOR**  
Settings > Monitoring > Window Services > Associate option.

Microsoft SQL usa le WMI per il monitoring

Per poter utilizzare VoIP monitor ci devono essere due router Cisco e su di questi deve essere abilitato IP SLA MONITOR (Cisco IOS >= 12.4)

**CCTV** permette di vedere solo specifiche dashboard in modo ripetitivo

**SNMP WALK** is an SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information.

**SNMP GET 🡪** ottenere valore inseguito ad una interrogazione di una variabile UDP-161 (RFC1213)  
**SNMP TRAP 🡪** il valore viene inviato dal client monitorato al server UDP-162 (RFC1215)  
**SNMP GETNEXT** 🡪 ottengo il valore dello OID successivo (usato da SNMP WALK)  
**SNMP BULK** 🡪 è una operazione introdotta con SNMPv2 e permette di ottenere in modo facile una grande quantità di dati con una singola richiesta SNMP.

**AD Manager Plus non si integra con OpManager**

I protocolli di crittografia usati per SNMPv3 sono DES e AES-128

Di default il discovery layer2 viene eseguito ogni 5 giorni